THE SMOOTH ENTROPY FORMALISM ON VON NEUMANN ALGEBRAS

MARIO BERTA

Institut für Theoretische Physik, ETH Zürich, Wolfgang-Pauli Strasse 27, 8093 Zürich
berta@phys.ethz.ch

FABIAN FURRER

Institut für Theoretische Physik, Leibniz Universität Hannover, Appelstrasse 2, 30167 Hannover
fabian.furrer@itp.uni-hannover.de

VOLKHER B. SCHOLZ

Institut für Theoretische Physik, Leibniz Universität Hannover, Appelstrasse 2, 30167 Hannover
volkher.scholz@itp.uni-hannover.de

Abstract. We discuss quantum information theoretical concepts on von Neumann algebras and lift the smooth entropy formalism to the most general quantum setting. For the smooth min- and max-entropies we recover similar characterizing properties and information-theoretic operational interpretations as in the finite-dimensional case. We generalize the entropic uncertainty relation with quantum side information of Tomamichel and Renner and sketch possible applications to continuous variable quantum cryptography. In particular, we prove the possibility to perform privacy amplification and classical data compression with quantum side information modeled by a von Neumann algebra. From this we generalize the formula of Renes and Renner characterizing the optimal length of a distillable secure finite-key. We also elaborate on the question when the formalism of von Neumann algebras is of advantage in the description of quantum systems with an infinite number of degrees of freedom.

Date: July 28, 2011.

Contents

1. Introduction

During the last decades many concepts and techniques have been developed to study quantum information-theoretical tasks using physical systems described by finite-dimensional Hilbert spaces. One of today's main conceptual building blocks is the smooth entropy formalism. In this paper, we begin to extend its scope to more general physical systems modeled by von Neumann algebras. The general aim is the development of a mathematical framework suited to describe quantum informational tasks with resources like bosonic or fermionic quantum fields. The motivation being the perspective to apply existing techniques to continuous variable protocols, where the focus lies on quantum cryptography.

A fundamental concept in classical and quantum information theory are entropy measures. They can be defined via an axiomatic approach [78], or operationally, in the sense that they quantitatively characterize fundamental tasks in information theory [84, 6, 83]. If the underlying resources are independent and identically distributed (iid), the relevant measure is the von Neumann entropy.[1] In the setting of von Neumann algebras, it was defined by Araki [3] and studied by Petz and coworkers [45, 65, 66, 46]. In order to analyze resources of general form, Renner et. al. developed the smooth entropy formalism [72, 75, 54, 89, 90, 32, 74]. The fundamental entropic quantities are the smooth conditional min- and max-entropy, quantifying the necessary resources for basic information theoretic tasks (cf. Section 2.2 for an overview). For iid resources the von Neumann entropy is then recovered in the asymptotic limit of infinitely many repetitions [89]. Furthermore, the smooth entropy formalism has also been applied to (quantum) statistical mechanics [30, 33].

In order to study information theoretic tasks for systems modeled by von Neumann algebras, we first recapitulate the notion of multipartite systems and discuss quantum information theoretic tools,

[1] The classical Shannon entropy of probability distributions can be seen as a special case of the von Neumann entropy.

like purification, in this mathematical formalism (Section 3). This enables us to define and study the smooth conditional min- and max-entropy, $\mathrm{H}_{\min}^{\epsilon}(A|B)$ and $\mathrm{H}_{\max}^{\epsilon}(A|B)$, in the setting of von Neumann algebras (Section 4). To be precise, we allow for an arbitrary von Neumann algebra to model the quantum side information B, while the system A is modeled by a finite-dimensional classical or quantum system. This is no restriction for questions regarding standard quantum cryptography, since there, the first system always becomes classical at some point.

But why is the setting of von Neumann algebras physically interesting? In quantum information theory one usually considers quantum systems which can be described by finite-dimensional Hilbert spaces, like for instance the polarization of a photon. But in many experimental setups one operates with physical systems which are modeled on infinite-dimensional Hilbert spaces. One important example are continuous variable systems in quantum optics, which are interesting candidates for implementations of various quantum information processing tasks (see e.g. [2] and references therein). In order to describe such systems it is often more accurate and mathematically more elegant to follow an algebraic approach based on von Neumann algebras (cf. Section 2.1 for a motivation). This formulation has the advantage that physical symmetries can readily be included into the algebraic structure.

In the special case that the von Neumann algebra is equal to the algebra of all linear, bounded operators on some Hilbert space, the smooth entropy formalism has been studied in [40]. It was shown that many results from the finite-dimensional case carry over via an inductive limit taken over all finite-dimensional subspaces. However, the assumption of a full algebra of all linear and bounded operators is often too restrictive. For example, the von Neumann algebra of a field of free bosons at finite temperature is not of this type [4].

The motivation of this work stems from questions in quantum key distribution, where rigorous mathematical proofs for security with continuous variable systems in the finite key regime are still absent (see e.g. [55]). Quantum key distribution is the art of generating a common secret key between two parties using communication over a (unknown) quantum channel and an authentic classical channel. In the finite-dimensional regime, the smooth conditional min- and max-entropy are known to quantify the relevant informational tasks like privacy amplification [72, 93] and classical data compression with (quantum) side information [75, 76, 70]. Using these tools, the security of many schemes against general attacks then follows via a quantum exponential de Finetti theorem [72, 71] or the post-selection technique [27]. But unfortunately these techniques fail in infinite-dimensional systems [26].

However, recently it was shown [92, 91] how to prove the security for a large class of quantum key distribution schemes by an entropic uncertainty relation with quantum side information, without making reference to a quantum exponential de Finetti theorem or the post-selection technique. In fact, since the early days of quantum key distribution, the intuition for security lies in the uncertainty principle [100, 7, 38]. But from the perspective of quantum cryptography the uncertainty cannot be treated as absolute, but has to be considered with respect to the prior knowledge of a quantum observer [101, 12]. In Section 6, we prove such an uncertainty relation, which is a direct generalization of the finite-dimensional result in [92]. Hence, in order to follow the analysis in [92, 91], it remains to generalize privacy amplification and classical data compression with quantum side information to our setup.

Privacy amplification is the art of extracting a perfect key from a source which might be correlated to a quantum adversary and is not perfectly random [93, 72]. We discuss this in Section 7, and show, as a generalization of the finite-dimensional result, that the smooth conditional min-entropy characterizes the amount of extractable key. This is also important for device-independent quantum cryptography, where the aim is to prove security solely based on the obtained measurement statistics (see e.g. [47, 56] and references therein). So far, it was often implicitly assumed that the adversary

is modeled by a finite-dimensional system in order to apply the results on privacy amplification, an assumption which can be dropped now.

In classical data compression with quantum side information one asks how much a classical message can be compressed, given that the receiver already has some quantum knowledge about it. In Section 8, we show that this task is characterized by the smooth conditional max-entropy, a result already known for the finite-dimensional case [70]. Afterwards privacy amplification and data compression are put together in Section 9, where we quantify the amount of distillable key for a given state; again along the lines of the finite-dimensional result [70]. We note that the detailed analysis of actual continuous variable quantum key distribution protocols is ongoing research, and that we do not give any security proofs here.

Let us again briefly summarize how the paper is organized. In Section 2.1, we discuss why it benefits to use a von Neumann algebra approach to describe continuous variable systems. The formalism of smooth min- and max-entropies and their use in quantum information theory is reviewed in Section 2.2. In Section 3, we begin with a brief introduction to von Neumann algebras, followed by a discussion of the relevant quantum information theoretical concepts on von Neumann algebras. We proceed with the definition of the smooth min- and max-entropies on von Neumann algebras in Section 4, and discuss some properties. In Section 5, we address the operational meanings of the 'non-smooth' min- and max-entropies. An uncertainty relation with quantum side information is proven in Section 6. The characterization of privacy amplification via the smooth min-entropy and data compression via the smooth max-entropy are derived in Section 7 and Section 8, respectively. This is followed by the discussion of an optimal quantum key distillation procedure in Section 9. We end with a summary of our results and a presentation of some perspectives concerning applications in Section 10.

2. Motivation

2.1. **Mathematical Models for Quantum Mechanics.** The usual description of a quantum system in quantum information theory is as follows. The basic object for every physical system is a separable, or often even finite-dimensional, Hilbert space $\mathcal{H}$ and states are described by density operators. These are linear, positive semi-definite operators ρ from $\mathcal{H}$ to itself with trace equal to one. The evolution is described by either an unitary transformation $U : \mathcal{H} \to \mathcal{H}$, or a measurement of an observable, which is given by a bounded, self-adjoint operator O on $\mathcal{H}$.[2] The expectation value of a measurement described by the observable O is computed as $\mathrm{Tr}(\rho O)$ if the system is in the state ρ. Multipartite systems are described by the unique tensor product of the Hilbert spaces of the individual systems.

In contrast to this, in general quantum theory, especially in quantum field theory, the basic object for every physical system is a von Neumann algebra $\mathcal{M}$ of observables. Based on the usual approach as given above, this can for example be motivated as follows. Starting with a Hilbert space $\mathcal{H}$, it is often the case that the physical system obeys certain symmetry conditions. Such symmetries can be due to the evolution determined by the Hamilton operator (dynamical symmetries) or postulated symmetries of the theory itself (superselection rules [42]). Typical examples are for instance Ising spin chains at zero temperature which are translational invariant, or bosonic systems which are invariant under particle permutation. Such symmetry constraints are realized by a representation π of the symmetry group G on $\mathcal{H}$, and the requirement that all observables O of the theory are invariant under group actions $g \in G$,

$$\pi(g^{-1})\, O\, \pi(g) = O \ ,$$

[2]There are more general ways to describe the evolution of a quantum system, which are introduced in Section 3.2. But for the following explanatory discussion this is sufficient.

which is the same as saying that all physical states are invariant. If the group acts reducibly on $\mathcal{H}$ it follows that not all mathematical possible observables can actually be observed. Hence, the set of physical observables form a subalgebra of the linear, bounded operators $\mathcal{B}(\mathcal{H})$ on $\mathcal{H}$. If $\mathcal{H}$ is infinite-dimensional, the imposed topological requirements on these subalgebras are, however, more subtle. Take a sequence O_i of observables such that $\mathrm{Tr}(\rho O_i)$ is a convergent sequence for all density operators ρ on $\mathcal{H}$. It is then physically reasonable to require that a 'limit' observable O exists which give rise to this value. In other words, we would require that the subalgebra of physical observables is closed with respect to taking expectation values. This topology is usually called the σ-weak (or weak*) topology and a σ-weakly closed *-subalgebra (invariant under taking the adjoint) of some $\mathcal{B}(\mathcal{H})$ is a von Neumann algebra $\mathcal{M}$. States in the Hilbert space sense, i.e. density operators ρ, now induce normalized, positive, normal (i.e. σ-weakly continuous) linear functionals $\omega_\rho : \mathcal{M} \to \mathbb{C}$ via

$$\omega_\rho(a) = \mathrm{Tr}(\rho a) \ ,$$

for $a \in \mathcal{M}$. The basic idea of the algebraic approach to quantum theory, is to think of the von Neumann algebra $\mathcal{M}$ as constructed above, as the fundamental object. States of the system are then described by linear, positive, normal, normalized functionals on $\mathcal{M}$.

We could also choose the norm topology to complete a *-subalgebra of $\mathcal{B}(\mathcal{H})$. This would then lead us to the definition of a C^*-algebra, which is more general than a von Neumann algebra. In particular, one often defines C^*-algebras independent of the particular representation, i.e. by just requiring certain invariance properties under group actions. Every representation of this invariance group is then defining a different physical setup, or one could say 'phase'. However, once one chooses such a representation, i.e. a Hilbert space $\mathcal{H}$, it is possible to close the observable algebra in the σ-weak topology and again end up with a von Neumann algebra. Hence, one could say that C^*-algebras are the abstract objects defining the theory, whereas von Neumann algebras correspond to 'physical realizations' of that theory.

Multipartite quantum systems are usually modeled by tensor products of Hilbert spaces, the basic idea being that the observables of different parties should not influence each other and therefore commute. Thus, multipartite quantum systems in our setting are described by a von Neumann algebra $\mathcal{M}_{ABC}$ with commuting subalgebras $\mathcal{M}_A, \mathcal{M}_B, \mathcal{M}_C$, such that the algebra generated by $\mathcal{M}_A \cup \mathcal{M}_B \cup \mathcal{M}_C$ is dense in $\mathcal{M}_{ABC}$. We note that such von Neumann algebras can not always be represented on product Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$. The question whether the possible correlations of multipartite systems modeled by commuting von Neumann algebras is richer than the one obtainable from systems with tensor product structure is an open question. For bipartite systems, this is known as Tsirelson's problem [94, 59, 52, 82, 58].[3] From the perspective of quantum cryptography, this means that the set of possible correlations using von Neumann algebras might be strictly larger then the set of possible correlations in the standard Hilbert space approach. Note however that the results of this paper suggest, that it actually does not matter for quantum cryptography if Tsirelson's problem has a positive or a negative solution, since all relevant results are proven to hold even in the more general setting (see in particular Sections 7 and 9).

The Hilbert space approach can be seen as a special case of the von Neumann algebra approach if the von Neumann algebra is isomorphic to a full $\mathcal{B}(\mathcal{H})$.[4] Such a von Neumann algebra is called

[3]It is known that Tsirelson's problem has an affirmative answer for a large class of physical systems, namely if the system's C^*-algebra is nuclear and/or if the corresponding von Neumann algebra is hyperfinite. But note that this is in general a non-constructive statement, that is, one only knows that there exists a bipartite Hilbert space which reproduces the correlations. In addition the Hilbert space might not be separable (see [82] for a detailed discussion).

[4]Even for finite-dimensional Hilbert spaces, a von Neumann algebra does not have to be a full $\mathcal{B}(\mathcal{H})$ (although it is always a direct sum of finite type I factors). But in quantum information theory, one usually just models every algebra of observables as a full $\mathcal{B}(\mathcal{H})$. In the spirit of cryptography, this assumption is reasonable in the sense that one does not want to restrict the eavesdropper's von Neumann algebra of observables in any way. But note that in the infinite-dimensional case, a restriction might be manifest because the von Neumann algebra is specified. See Section 7 for a detailed discussion.

a factor of type I and in this case - but only then - it is possible to use techniques as in [40]. But there are many von Neumann algebras occurring in physics which are not of such type. For example, a free boson field of finite temperature [4]. Here the invariance under particle permutation is the restricting symmetry. Another example of a non-type I factor are the algebras typically assumed to model the set of observables corresponding to a finite space-time region in algebraic quantum field theory [18].

We conclude therefore that the von Neumann algebra approach is mathematically more general than the standard one using Hilbert spaces, and in favor because it is a unified framework for regular quantum mechanics, quantum statistical mechanics and quantum field theory. In Section 3, we give a concise introduction of this mathematical framework.

2.2. **The Smooth Entropy Formalism.** This section contains a review of previously existing finite-dimensional results. The general framework for the von Neumann algebra setting is developed in Sections 4 - 6.

In quantum information theory, and especially in quantum cryptography, one is interested in multipartite systems. Concerning entropies, this means that one needs conditional measures. For bipartite systems AB, the smooth conditional min-entropy $\mathrm{H}_{\min}^{\epsilon}(A|B)_{\rho}$ and the smooth conditional max-entropy $\mathrm{H}_{\max}^{\epsilon}(A|B)_{\rho}$ were introduced in [72, 54, 90]. These measures depend on the state ρ_{AB} of the system and on a smoothing parameter $\epsilon \geq 0$, which typically corresponds to an error tolerance in information theoretic operational interpretations. The smooth min- and max-entropy are considered as reasonable measures, because on one hand, they have many properties that are desirable for entropies, and on the other hand they quantitatively characterize basic information theoretic tasks. In fact, these two points should really be seen as the justification for their definition.

For $\epsilon = 0$, the conditional min-entropy corresponds to the maximum achievable overlap with a maximally entangled state if only local operations on the part B are allowed, and the conditional max-entropy is related to the maximum fidelity with a product state that is completely mixed on A [54]. In the von Neumann algebra setting this corresponds to Corollary 5.1 and Proposition 5.5. Another basic property that we would like to highlight here, is a useful duality relation between the two entropies. For a tripartite pure state ρ_{ABC} and $\epsilon \geq 0$ it holds that [90]

$$\mathrm{H}_{\min}^{\epsilon}(A|B)_{\rho} = -\mathrm{H}_{\max}^{\epsilon}(A|C)_{\rho} \ .$$

Based on this relation, one can derive an entropic uncertainty relation with quantum side information [92], which corresponds to Theorem 6.1 in the von Neumann algebra setting.

The smooth min- and max-entropies appear in information theoretic tasks like data compression [75, 76, 70], channel coding problems [37, 11, 77, 57, 22, 97, 69, 50], and privacy amplification [72, 93]. Moreover, similar quantities are used in entanglement theory [31, 21, 20, 23, 15]. Even though, the smooth min- and max-entropies are suited to study resources of general form, they are also useful as a technical tool to study iid resources [12, 13]. This is because the von Neumann entropy is a special case of the smooth min- and max-entropy, which is established via the fully quantum asymptotic equipartition property [89].

3. Preliminaries

Here we introduce the notation and the mathematical tools needed to describe quantum physics in the framework of von Neumann algebras. In Section 3.1, we introduce the basic mathematical objects and fix some notation, whereas in Section 3.2, we address the description of quantum mechanics in this framework. Among others, we define basic information theoretic notions like purifications, and also discuss special type of systems in greater detail. These are bipartite systems AB, where A is a finite-dimensional classical or quantum system and B is a system modeled by an arbitrary von Neumann algebra.

3.1. **An Introduction to von Neumann Algebras.** This section is aimed to give a brief but, as far as possible, self-contained mathematical introduction to the theory of von Neumann algebras and the concepts used within this paper. For a more sophisticated introduction and further literature we refer to [16, 17, 86, 87, 88].

A $*$-algebra is an algebra $\mathcal{A}$ which is also a vector space over $\mathbb{C}$, together with an operation $*$ called involution, which satisfies the property $A^{**} = A$, $(AB)^* = B^*A^*$ and $(\alpha A + \beta B)^* = \bar{\alpha}A^* + \bar{\beta}B^*$ for all $A, B \in \mathcal{A}$ and $\alpha, \beta \in \mathbb{C}$. If a $*$-algebra is equipped with a norm for which it is complete, it is called a Banach $*$-algebra.

Definition 3.1. *A C^*-algebra is a Banach $*$-algebra $\mathcal{A}$ with the property*

$$\|A^*A\| = \|A\|^2 \ , \tag{1}$$

for all $A \in \mathcal{A}$.

Henceforth, $\mathcal{A}$ always denotes a C^*-algebra if nothing else mentioned. Note that the set of all linear, bounded operators on a Hilbert space $\mathcal{H}$, denoted by $\mathcal{B}(\mathcal{H})$, is a C^*-algebra with the usual operator norm (induced by the norm on $\mathcal{H}$), and the adjoint operation. Furthermore, each norm closed $*$-subalgebra of $\mathcal{B}(\mathcal{H})$ is a C^*-algebra.

A representation of a C^*-algebra $\mathcal{A}$ is a $*$-homomorphism $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ on a Hilbert space $\mathcal{H}$. A $*$-homomorphism is a linear map compatible with the $*$-algebraic structure, that is, $\pi(AB) = \pi(A)\pi(B)$ and $\pi(A^*) = \pi(A)^*$. We call a representation π faithful if it is an isometry, which is equivalent to say that it is a $*$-isomorphism from $\mathcal{A}$ to $\pi(\mathcal{A})$. A basic theorem in the theory of C^*-algebras says that each $\mathcal{A}$ is isomorphic to a norm closed $*$-subalgebra of a $\mathcal{B}(\mathcal{H})$ with suitable $\mathcal{H}$ [16, Theorem 2.1.10]. Hence, each C^*-algebra can be seen as a norm closed $*$-subalgebra of a $\mathcal{B}(\mathcal{H})$.

An element $b \in \mathcal{A}$ is called positive if $b = a^*a$ for $a \in \mathcal{A}$, and the set of all positive elements is denoted by $\mathcal{A}_+$. A linear functional ω in the dual space $\mathcal{A}^*$ of $\mathcal{A}$ is called positive if $\omega(a) \geq 0$ for all $a \in \mathcal{A}_+$. The set of all positive functionals $\mathcal{A}^*_+$ defines a positive cone in $\mathcal{A}^*$ with the usual ordering $\omega_1 \geq \omega_2$ if $(\omega_1 - \omega_2) \in \mathcal{A}^*_+$, and we say that ω_1 majorizes ω_2. A positive functional $\omega \in \mathcal{A}^*$ with $\|\omega\| = 1$ is called a state. The norm on the dual space of $\mathcal{A}$ is defined to be

$$\|\omega\| = \sup_{x \in \mathcal{A}, \|x\| \leq 1} |\omega(x)| \ . \tag{2}$$

A state ω is called pure if the only positive linear functionals which are majorized by ω are given by $\lambda \cdot \omega$ for $0 \leq \lambda \leq 1$. If $\mathcal{A} = \mathcal{B}(\mathcal{H})$ we have that the pure states are exactly the functionals $\omega_\xi(x) = \langle \xi \, | x\xi \, \rangle$, where $|\xi\rangle \in \mathcal{H}$.

Now we consider a subset of linear, bounded operators $\mathcal{T} \subset \mathcal{B}(\mathcal{H})$ on a Hilbert space $\mathcal{H}$. The commutant $\mathcal{T}'$ of $\mathcal{T}$ is defined as $\mathcal{T}' = \{a \in \mathcal{B}(\mathcal{H}) : [a, x] = 0, \forall \, x \in \mathcal{T}\}$.

Definition 3.2. *Let $\mathcal{H}$ be a Hilbert space. A von Neumann algebra $\mathcal{M}$ acting on $\mathcal{H}$ is a $*$-subalgebra $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$ which satisfies $\mathcal{M}'' = \mathcal{M}$.*

There are three other characterizations of a von Neumann algebra. One rises in the bicommutant theorem [16, Lemma 2.4.11]: a $*$-subalgebra $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$ containing the identity is σ-weakly closed if and only if $\mathcal{M}'' = \mathcal{M}$.[5] From this we can conclude that a von Neumann algebra $\mathcal{M}$ is also norm closed and therefore a C^*-algebra.[6] The definition of a von Neumann algebra can even be stated in the category of C^*-algebras: a von Neumann algebra $\mathcal{M}$ is a C^*-algebra with the property that it is the dual space of a Banach space. Due to historical reasons this is also called a W^*-algebra.

[5]The σ-weak topology on $\mathcal{B}(\mathcal{H})$ is the locally convex topology induced by the semi-norms $A \mapsto |\mathrm{Tr}(\tau A)|$ for trace-class operators $\tau \in \mathcal{B}(\mathcal{H})$, see [16, Chapter 2.4.1].

[6]We note that a norm closed subalgebra is not necessarily σ-weakly closed. Thus a C^*-algebra on $\mathcal{H}$ is not always a von Neumann algebra.

In the following $\mathcal{M}$ denotes a von Neumann algebra. We call $\mathcal{Z}(\mathcal{M}) = \mathcal{M} \cap \mathcal{M}'$ the center of $\mathcal{M}$ and $\mathcal{M}$ a factor if $\mathcal{Z}(\mathcal{M})$ consists only of multiples of the identity. A representation π of a von Neumann algebra $\mathcal{M}$ is a $*$-representation on a Hilbert space $\mathcal{H}$ that is σ-weakly continuous. Thus, the image $\pi(\mathcal{M})$ is again a von Neumann algebra. We say that two von Neumann algebras are isomorphic if there exists a faithful representation mapping one into the other.

A linear functional $\omega : \mathcal{M} \to \mathbb{C}$ is called normal if it is σ-weakly continuous and we denote the set of linear, normal functionals on $\mathcal{M}$ by $\mathcal{N}(\mathcal{M})$.[7] We equip $\mathcal{N}(\mathcal{M})$ with the usual norm as given in (2). Then the set $\mathcal{N}(\mathcal{M})$ is a Banach space and moreover it is the predual of $\mathcal{M}$, which means that its dual space is $\mathcal{M}$. The cone of positive elements in $\mathcal{N}(\mathcal{M})$ is denoted by $\mathcal{N}^+(\mathcal{M})$.[8] It is worth to mention that $\|\omega\| = \omega(\mathbb{1})$ for all $\omega \in \mathcal{N}^+(\mathcal{M})$. We call functionals $\omega \in \mathcal{N}^+(\mathcal{M})$ with the property $\|\omega\| \leq 1$ subnormalized states and denote the set of all subnormalized states by $\mathcal{S}_{\leq}(\mathcal{M})$. Moreover, we say that $\omega \in \mathcal{S}_{\leq}(\mathcal{M})$ is a normalized state if $\|\omega\| = 1$, and set $\mathcal{S}(\mathcal{M}) = \{\omega \in \mathcal{S}_{\leq}(\mathcal{M}) : \|\omega\| = 1\}$. For $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$, we have that $\omega \in \mathcal{S}_{\leq}(\mathcal{M})$ corresponds to the functionals for which a positive trace-class operator ρ on $\mathcal{H}$ exists, such that

$$\omega_\rho(x) = \mathrm{Tr}(\rho x) = \omega(x) \ \forall x \in \mathcal{M} \ . \tag{3}$$

Such an operator ρ is called a density operator.

Given two commuting von Neumann algebras $\mathcal{M}$ and $\hat{\mathcal{M}}$ acting on the same Hilbert space $\mathcal{H}$, we define the von Neumann algebra generated by $\mathcal{M}$ and $\hat{\mathcal{M}}$ as $\mathcal{M} \vee \hat{\mathcal{M}} = (\mathcal{M} \cup \hat{\mathcal{M}})''$, where $\mathcal{M} \cup \hat{\mathcal{M}} = \mathrm{span}\{\mathrm{xy} \ ; \ \mathrm{x} \in \mathcal{M}, \mathrm{y} \in \hat{\mathcal{M}}\}$. According to the bicommutant theorem [16, Lemma 2.4.11], $\mathcal{M} \vee \hat{\mathcal{M}}$ is just the σ-weak closure of $\mathcal{M} \cup \hat{\mathcal{M}}$.

3.2. **Quantum Information Theory on von Neumann Algebras.** For motivations of the following description we refer to Section 2.1 and references therein. We associate with every physical system a von Neumann algebra $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$, which is generated by the possible observables on this system. An observable is given by a positive operator valued measure (POVM), which consists of a measurable space (X, Σ) with σ-algebra Σ defining the values of the possible measurement outcomes together with an additive function $E : \Sigma \to \mathcal{M}_+$ such that $E(X) = \mathbb{1}$. Henceforth, we consider only observables with a finite number of measurement outcomes $X = \{1, 2, ..., n\}$, which are then described by operators $0 \leq E_x \leq \mathbb{1}$ in $\mathcal{M}$ with the property $\sum_x E_x = \mathbb{1}$. A measurement is called projective or of von Neumann type if the operators E_x are projections. A state of the physical system is described by a functional $\omega \in \mathcal{S}(\mathcal{M})$. Given that we perform a measurement described by $\{E_x\}$ on a system in the state ω, the probability to measure the outcome x is $\omega(E_x)$.

The maps that describe possible evolutions of quantum systems are called quantum channels. A quantum channel from system A to system B described by von Neumann algebras $\mathcal{M}_A$ and $\mathcal{M}_B$, respectively, is a normal, completely positive, unital, linear map $\mathcal{E} : \mathcal{M}_B \to \mathcal{M}_A$ (see [62] for proper definitions of these terms). Hence, if we prepare a system in the state $\omega \in \mathcal{S}(\mathcal{M}_A)$, apply a quantum channel $\mathcal{E} : \mathcal{M}_B \to \mathcal{M}_A$, and measure the observable $\{E_x\}_{x \in X}$, this yields a probability distribution $p(x) = \omega(\mathcal{E}(E_x))$. We can define the dual map $\mathcal{E}_* : \mathcal{N}(\mathcal{M}_A) \to \mathcal{N}(\mathcal{M}_B)$ via the relation $\mathcal{E}_*(\omega)(a) = \omega(\mathcal{E}(a))$ for all $a \in \mathcal{M}_B$. $\mathcal{E}_*$ then maps states onto states. Since $\mathcal{N}(\mathcal{M})^* = \mathcal{M}$ these maps are dual to each other.

A multipartite system is a composite of different physical subsystems $A, B, \ldots, Z$ associated with mutually commuting von Neumann algebras $\mathcal{M}_A, \mathcal{M}_B, \ldots, \mathcal{M}_Z$ of corresponding observables acting on the same Hilbert space $\mathcal{H}$.[9] The commutation relation comes from the assumption that the

[7] In standard von Neumann algebra notation $\mathcal{N}(\mathcal{M})$ corresponds to the set $\mathcal{M}_*$.

[8] In standard von Neumann algebra notation $\mathcal{N}^+(\mathcal{M})$ corresponds to the set $\mathcal{M}_*^+$.

[9] We can always assume that the von Neumann algebras act on the same Hilbert space. Otherwise, if $\mathcal{M}_A \subset \mathcal{B}(\mathcal{H}_A)$ and $\mathcal{M}_B \subset \mathcal{B}(\mathcal{H}_B)$, we consider the algebraic tensor product $\mathcal{M}_A \otimes \mathcal{M}_B \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$, and take the σ-weak closure of $\mathcal{M}_A \otimes \mathcal{M}_B$ in $\mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$, which is equivalent to $(\mathcal{M}_A \otimes \mathbb{1}) \vee (\mathbb{1} \otimes \mathcal{M}_B)$.

subsystems are in space-like separated areas before performing measurements on single subsystems. The overall system denoted by $\mathcal{M}_{AB\ldots Z}$ is then given by the von Neumann algebra generated by the individual systems

$$\mathcal{M}_{AB\ldots Z} = \mathcal{M}_A \vee \mathcal{M}_B \vee \ldots \vee \mathcal{M}_Z \ . \tag{4}$$

Throughout this paper we use the notation $\mathcal{M}_{ABC}$ to indicate that we consider a multipartite system consisting of subsystems $\mathcal{M}_A, \mathcal{M}_B$ and $\mathcal{M}_C$. For states on multipartite systems, the considered subsystems are indicated by subscripts. For example, a state on $\mathcal{M}_{ABC}$ is usual denoted by ω_{ABC} while ω_{AB} is the restriction of ω_{ABC} onto $\mathcal{M}_{AB}$.

An important concept in quantum information theory is 'purification', which is essentially the completion of a system by adding a 'complementary' system. Assume that we have a state ω_A on a von Neumann algebra $\mathcal{M}_A$. This state may be regarded as a state ω on a bigger von Neumann algebra $\mathcal{M}$, which contains $\mathcal{M}_A$ as a subalgebra, provided the restriction of ω onto $\mathcal{M}_A$ is ω_A. Now the idea of purification is to choose an extension ω of ω_A such that ω is pure. The name is justified by the property that no further extension of the system shows any correlation with the purification ω [87, Section IV, Lemma 4.11]: if $\tilde{\omega} \in \mathcal{S}(\tilde{\mathcal{M}})$ with $\mathcal{M} \subset \tilde{\mathcal{M}}$ and $\tilde{\omega}$ restricted to $\mathcal{M}$ is a pure state ω on $\mathcal{M}$, then it follows that $\tilde{\omega}(xy) = \tilde{\omega}(x)\tilde{\omega}(y)$ for all $x \in \mathcal{M}$ and $y \in \mathcal{M}' \cap \tilde{\mathcal{M}}$.

Definition 3.3. *Let $\mathcal{M}$ be a von Neumann algebra and $\omega \in \mathcal{S}_\leq(\mathcal{M})$. A purification of ω is defined as a triple $(\pi, \mathcal{H}, |\xi\rangle)$, where π is a representation of $\mathcal{M}$ on a Hilbert space $\mathcal{H}$, and $\xi \in \mathcal{H}$ is such that $\omega(x) = \langle \xi \, | \pi(x) \xi \, \rangle$ for all $x \in \mathcal{M}$. Moreover, we call $\pi(\mathcal{M})$ the relevant and $\pi(\mathcal{M})'$ the complementary system of the purification $(\pi, \mathcal{H}, |\xi\rangle)$.*

Introducing a little abuse of notation, we say for short that $\omega_{A'B}$ is a purification of $\omega_A \in \mathcal{S}_\leq(\mathcal{M}_A)$, if there exists a purification $(\pi, \mathcal{H}, |\xi\rangle)$ of ω_A such that $\mathcal{M}_{A'} = \pi(\mathcal{M}_A)$, $\mathcal{M}_B = \pi(\mathcal{M}_A)'$ and $\omega_{A'B}(x) = \langle \xi \, | x \xi \, \rangle$ for all $x \in \mathcal{M}_{A'B}$. Note that such a purification $\omega_{A'B}$ is in general not a pure state on $\mathcal{M}_{A'B}$, although the vector state $\omega_\xi(x) = \langle \xi \, | x \xi \, \rangle$ on $\mathcal{B}(\mathcal{H})$ is. This complication arises naturally when defining a purification of states on von Neumann algebras, because the only states for which pure extensions on $\mathcal{M}_{AB}$ exist are factor states [102].[10] Another important property of a purification $(\pi, \mathcal{H}, |\xi\rangle)$ of $\omega_A \in \mathcal{S}(\mathcal{M}_A)$ is that π is not required to be faithful on the entire $\mathcal{M}_A$ but only on the part 'seen' by the state ω_A. This means that $\mathcal{M}_A$ is in general not isomorphic to $\pi(\mathcal{M}_A)$ and the systems cannot be identified, wherefore we denoted $\pi(\mathcal{M}_A)$ by A' instead of A. Beside the mathematical convenience, this is justified because a purification is just a theoretical construct without direct physical relevance, and can therefore chosen to be state dependent.[11] It is worth to mention that, we can choose for any von Neumann algebra $\mathcal{M}$ a particular representation π on a Hilbert space $\mathcal{H}$, such that every state on $\mathcal{M}$ has a purification in $\mathcal{H}$. This specific representation is called the standard form of $\mathcal{M}$ (see Appendix A), and ensures that any state has a purification. Moreover, by the Gelfand-Naimark-Segal (GNS) construction [16, Section 2.3.3] we can choose the purification $(\pi, \mathcal{H}, |\xi\rangle)$ of $\omega \in \mathcal{M}$ to be cyclic, that is, $\mathcal{H}$ is the closure of $\{\pi(x)|\xi\rangle : x \in \mathcal{M}\}$. A purification is therefore not unique, but all possible ones are connected by partial isometries.

Lemma 3.4. *Let $\mathcal{M}$ be a von Neumann algebra, $\omega \in \mathcal{S}_\leq(\mathcal{M})$, and $(\pi_i, \mathcal{H}_i, |\xi_i\rangle)$ with $i = 1, 2$ two purifications of ω. Then there exists a partial isometry $V : \mathcal{H}_1 \to \mathcal{H}_2$ such that $V|\xi_1\rangle = |\xi_2\rangle$ and V intertwines with the representations π_i, that is, $V\pi_1(x) = \pi_2(x)V$ for all $x \in \mathcal{M}$.*

Proof. We construct an explicit partial isometry V. Define V on $\{\pi_1(x)|\xi_1\rangle : x \in \mathcal{M}\}$ via $V\pi_1(x)|\xi_1\rangle = \pi_2(x)|\xi_2\rangle$. This defines V uniquely on the closed subspace $\mathcal{H}_1^\omega \subset \mathcal{H}_1$ given by the closure of $\{\pi_1(x)|\xi_1\rangle : x \in \mathcal{M}\}$. On the orthogonal complement of $\mathcal{H}_1^\omega$, we set V equal to zero. One can now verify that the constructed V satisfies the required properties. □

[10] A factor state is a state for which the Gelfand-Naimark-Segal (GNS) representation is a factor (see [16, Section 2.3.3] for the GNS construction). The reason why pure extensions exist only for such states, is due to the fact that the GNS construction of a pure state is a factor and $(\mathcal{M}_A \vee \mathcal{M}_B)'$ is equal to the center $\mathcal{Z}(\mathcal{M}_A)$.

[11] In finite dimension, a purification is often chosen to be state dependent as well. Given a density operator ρ_A on a Hilbert space $\mathcal{H}_A$, a purification of ρ_A is a rank one density operator $\rho_{A'B}$ on some Hilbert space $\mathcal{H}_{A'} \otimes \mathcal{H}_B$, such that $\rho_{A'} = \rho_A$. But note that $|A| \geq |A'| \geq \mathrm{rank}(\rho_A)$, and not necessarily $|A'| = |A|$.

We now discuss bipartite systems $\mathcal{M}_{AB}$, where the system A is either classical with a finite alphabet, or quantum with finite dimension.

Finite-Dimensional System A. For an arbitrary set $\mathcal{T}$, we denote by $M_n(\mathcal{T})$ the $n \times n$-matrices with entries in $\mathcal{T}$, and set $M_n = M_n(\mathbb{C})$. A n-dimensional quantum system is defined as the von Neumann algebra M_n.[12] We are therefore interested in bipartite systems $\mathcal{M}_{AB} = \mathcal{M}_A \vee \mathcal{M}_B$ with $\mathcal{M}_A \cong M_n$, and hence $\mathcal{M}_{AB} \cong M_n \otimes \mathcal{M}_B$.[13] An arbitrary element $x \in M_n \otimes \mathcal{M}_B$ can be written as $x = \sum_{ij} E_{ij} \otimes x_{ij}$, with $E_{ij} \in M_n$ the matrix with entry 1 at (i,j) and 0 elsewhere, and $x_{ij} \in \mathcal{M}_B$. This allows us to identify $M_n \otimes \mathcal{M}_B$ with $M_n(\mathcal{M}_B)$ via $x = (x_{ij})$, where (x_{ij}) denotes the matrix with entry x_{ij} at (i,j). In standard 'bra-ket' notation, E_{ij} corresponds to the rank one element $|i\rangle\langle j|$, where $|i\rangle_{1,\ldots,n}$ denotes an orthonormal bases of $\mathbb{C}^n$. We will freely use both of these notations throughout the paper. The similar fact holds for normalized states ω_{AB} on $\mathcal{M}_{AB}$ in the sense that $\mathcal{N}(M_n(\mathcal{M}_B))$ can be identified with $M_n(\mathcal{N}(\mathcal{M}_B))$. We use the notation $\omega_{AB} = (\omega_B^{ij})$, where $\omega_B^{ij}(b) = \omega_{AB}(E_{ij} \otimes b)$ for all $b \in \mathcal{M}_B$ and thus, obtain $\omega_{AB}(x) = \sum_{ij} \omega_B^{ij}(x_{ij})$ for $x = (x_{ij})$.

We briefly note that the states on $M_n(\mathcal{M}_B)$ are in one-to-one correspondence with completely positive maps from $\mathcal{M}_B$ onto M_n via the map $\omega_{AB} \mapsto \Phi_\omega$, defined by $(\Phi_\omega(b))_{ij} = \omega_B^{ij}(b)$, and its inverse $\Phi \mapsto \omega_{AB}^\Phi$ given by $\omega_{AB}^\Phi((x_{ij})) = \sum_{ij} \Phi(x_{ij})$ [62, Chapter 6].

Classical-Quantum States. A classical system in the context of quantum systems, is specified by the property that all possible observables commute, and is thus described by an abelian von Neumann algebra. In this paper we restrict to classical systems over a finite alphabet X. These are then given by the bounded complex valued functions on X, denoted by $\ell^\infty(X) = \ell^\infty(X, \mathbb{C})$. Elements in $\ell^\infty(X)$ can be represented as finite sequences $(\lambda_x)_{x \in X}$, and the norm is the supremum norm. Henceforth, we denote a classical system with alphabet X simply by X (instead of A), and also use the abbreviation $\ell_{|X|}^\infty$ for $\ell^\infty(X)$.

A bipartite system consisting of a classical part X, and a quantum part B, is then described by the von Neumann algebra $\mathcal{M}_{XB} = \ell_{|X|}^\infty \otimes \mathcal{M}_B$. This can be identified with the set of finite sequences $(a_x)_{x \in X}$, $a_x \in \mathcal{M}_B$, equipped with the norm

$$\|(a_x)\|_{\ell^\infty(\mathcal{M}_B)} = \sup_{x \in X} \|a_x\|_{\mathcal{M}_B} \ , \tag{5}$$

denoted by $\ell_{|X|}^\infty(\mathcal{M}_B) = \ell^\infty(X, \mathcal{M}_B)$. The set of normal functionals on $\ell_{|X|}^\infty \otimes \mathcal{M}_B$ is $\ell_{|X|}^1 \otimes \mathcal{N}(\mathcal{M}_B)$. States on $\ell_{|X|}^\infty \otimes \mathcal{M}_B$ are called classical quantum (cq-) states, and can be written as $\omega_{XB} = (\omega_B^x)_{x \in X}$, where $\omega_B^x \in \mathcal{S}_\leq(\mathcal{M}_B)$ such that $\omega_{XB}(a) = \sum_x \omega_B^x(a_x)$ for all $a = (a_x) \in \mathcal{M}_{XB}$. The norm inherited from $\ell_{|X|}^1 \otimes \mathcal{N}(\mathcal{M}_B)$ is then given by

$$\|(\omega^x)\|_{\ell^1(\mathcal{N}(\mathcal{M}_B))} = \sum_{x \in X} \|\omega^x\|_{\mathcal{N}(\mathcal{M}_B)} \ . \tag{6}$$

Note that $\ell_{|X|}^\infty \otimes \mathcal{M}_B$ can be identified with $\bigoplus_{x \in X} \mathcal{M}_B$, and that states can be written as $\omega_{XB} = \oplus_{x \in X} \omega_B^x$. Hence, we can think of $\ell_{|X|}^\infty(\mathcal{M}_B)$ as embedded into the quantum system $M_n(\mathcal{M}_B)$ as the algebra of diagonal matrices with entries in $\mathcal{M}_B$. Technically, this allows us to treat classical systems as subparts of quantum systems. In this spirit, we understand all the definitions made for quantum systems also for classical systems.

Cq-states can be interpreted as post-measurement states, where the outcome is treated as a random variable. Since we consider only measurements with finite alphabets, the classical part of the resulting

[12] This corresponds to a full algebra of observables $\mathcal{B}(\mathbb{C}^n)$. As discussed in Section 2, not every finite dimensional von Neumann algebra has this form, although one always (implicitly) makes this assumption in quantum information theory. In the following we also make this restriction for the system A, because the restriction is not relevant for quantum cryptography; the relevant part concerns the system B.

[13] Since M_n is finite-dimensional, and thus nuclear, the tensor product is uniquely defined.

cq-state is finite. Let us assume that we start with a bipartite state $\omega_{AB} \in \mathcal{S}(\mathcal{M}_{AB})$ on which we perform a measurement on the system A represented by the observable $\{E_x\}_{x\in X} \subset \mathcal{M}_A$. The normalized post-measurement states on $\mathcal{M}_B$ conditioned on the outcome $x \in X$, are described by $\frac{1}{\omega_B^x(\mathbb{1})}\omega_B^x$, where $\omega_B^x(a) = \omega_{AB}(E_x a)$ for all $a \in \mathcal{M}_B$. Note that $\omega_B^x(\mathbb{1})$ is just the probability to measure the outcome x. Hence, if we treat the outcome as a random variable, the post-measurement state is the cq-state $\omega_{XB} = (\omega_B^x)_{x\in X}$. The map $\omega_{AB} \mapsto (\omega_B^x)_{x\in X}$ describes a quantum channel from $\mathcal{M}_A$ to the classical output space $\ell_{|X|}^\infty$. Conversely, for any cq-state $\omega_{XB} = (\omega_B^x)_{x\in X}$ on $\mathcal{M}_{XB}$, we can find a state $\omega_{AB} \in \mathcal{S}(\mathcal{M}_A \vee \mathcal{M}_B)$ with suitable $\mathcal{M}_A$ and an observable $\{E_x\} \subset \mathcal{M}_A$, which give rise to ω_{XB}. The measurement operators E_x can for instance be chosen as the non-commutative Radon-Nikodym derivative of ω_B^x with respect to $\sum_x \omega_B^x$ (see Appendix B).

4. Smooth Entropies on von Neumann Algebras

Throughout this section, we indicate multipartite systems with subscripts $A, B, \ldots$ where the associated von Neumann algebras are $\mathcal{M}_A, \mathcal{M}_B, \ldots$ The system A is always given by a finite-dimensional matrix algebra $\mathcal{M}_A = M_n$, while the other von Neumann algebras are arbitrary. The definitions for a classical system with a finite alphabet X are obtained from the quantum case via the natural embedding into $M_{|X|}$ as the subalgebra of diagonal matrices with respect to a fixed basis.

4.1. Min- and Max-Entropies.

Similarly to the finite-dimensional case, the concept of relative entropy is very useful [60]. The following generalizes one of the main definitions in [31] to the von Neumann algebra setting.

Definition 4.1. *Let $\omega, \sigma \in \mathcal{N}^+(\mathcal{M})$. The max-relative entropy of ω with respect to σ is defined as*

$$\mathrm{D}_{\max}(\omega \,||\, \sigma) = \inf\{\mu \in \mathbb{R} : \omega \leq 2^\mu \cdot \sigma\} \ . \tag{7}$$

The max-relative entropy of ω with respect to σ is ∞ whenever the condition $\omega \leq 2^\mu \cdot \sigma$ can not be satisfied for any $\mu \in \mathbb{R}$. This is the case if the support of ω does not lie in the support of σ. The max-relative entropy can be reformulated in an operational way as[14]

$$\mathrm{D}_{\max}(\omega \,||\, \sigma) = \sup\{\log \omega(E) : E \in \mathcal{M}_+, \sigma(E) = 1\} \ .$$

In order to see this, one uses that $\omega \leq 2^\mu \cdot \sigma$ means by definition that $\omega(E) \leq 2^\mu \sigma(E)$ for all $E \in \mathcal{M}_+$. But this is equivalent to $\omega(E) \leq 2^\mu$ for all $E \in \mathcal{M}_+$ with $\sigma(E) = 1$.

Based on the relative max-entropy we define the conditional min-entropy in analogy to the finite-dimensional case [72, 54].

Definition 4.2. *Let $\mathcal{M}_{AB} = M_n \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra, and $\omega_{AB} \in \mathcal{S}_\leq(\mathcal{M}_{AB})$. The min-entropy of ω_{AB} conditioned on B is defined as*

$$\mathrm{H}_{\min}(A|B)_\omega = \sup_{\sigma_B \in \mathcal{S}(\mathcal{M}_B)} \{-\mathrm{D}_{\max}(\omega_{AB} \,||\, \tau_A \otimes \sigma_B)\} \ , \tag{8}$$

where τ_A denotes the trace on M_n, i.e. $\tau_A(x) = \mathrm{Tr}(x)$ for all $x \in M_n$.

Using the concept of purification on von Neumann algebras as introduced in Definition 3.3, we define the conditional max-entropy as the dual of the conditional min-entropy (as in [54, 90] for the finite dimensional case).

Definition 4.3. *Let $\mathcal{M}_{AB} = M_n \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra, and $\omega_{AB} \in \mathcal{S}_\leq(\mathcal{M}_{AB})$. The max-entropy of ω_{AB} conditioned on B is defined as*

$$\mathrm{H}_{\max}(A|B)_\omega = -\mathrm{H}_{\min}\left(A'|C\right)_\omega , \tag{9}$$

with $\omega_{A'B'C}$ given by an arbitrary purification $(\pi, \mathcal{K}, |\xi\rangle)$ of ω_{AB} with $\mathcal{M}_{A'B'} = \pi(\mathcal{M}_{AB})$ the relevant system, and $\mathcal{M}_C = \pi(\mathcal{M}_{A'B'})'$ the complementary system.

[14] From now on, we denote the logarithm of base two by log.

For simplicity, we often use a purification $(\pi, \mathcal{K}, |\xi\rangle)$ such that $\pi(\mathcal{M}_A)$ is isomorphic to $\mathcal{M}_A$, and simply write $\mathcal{M}_A$ for $\pi(\mathcal{M}_A)$. The next Lemma shows that the conditional max-entropy is well defined, that is, independent of the choice of the purification.

Lemma 4.4. *Let $\mathcal{M}_{AB} = M_n \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra, $\omega_{AB} \in \mathcal{S}_\leq(\mathcal{M}_{AB})$, and $(\pi_i, \mathcal{K}_i, |\xi_i\rangle)$ with $i = 1, 2$ two purifications of ω_{AB} with $\pi_i(\mathcal{M}_A) = \mathcal{M}_{A_i}$ and complementary systems $\mathcal{M}_{C_i}$. Then*

$$\mathrm{H}_{\min}\left(A_1|C_1\right)_{\omega^1} = \mathrm{H}_{\min}\left(A_2|C_2\right)_{\omega^2} \ , \tag{10}$$

where $\omega^i_{A_iC_i}$ is the restricted state corresponding to $|\xi_i\rangle$.

Proof. The conceptual idea for the proof is from [90, Lemma 13]. According to Lemma 3.4 we know that there exists a partial isometry $V : \mathcal{K}_1 \to \mathcal{K}_2$ with $|\xi_2\rangle = V|\xi_1\rangle$ and $V\pi_1(a) = \pi_2(a)V$ for all $a \in \mathcal{M}_{AB}$. Then it follows for all $x \in \mathcal{M}_{A_2} \otimes \mathcal{M}_{C_2}$ that

$$\omega^2_{A_2C_2}(x) = \langle \xi_2 \, | x \xi_2 \, \rangle = \langle \xi_1 \, | V^* x V \xi_1 \, \rangle = \omega^1_{A_1C_1}(V^* x V) \ , \tag{11}$$

where we used in the last equality that $V^*xV \in \mathcal{M}_{A_1} \otimes \mathcal{M}_{C_1}$. This follows from the fact that $(\mathcal{M}_{A_i} \otimes \mathcal{M}_{C_i})' = \pi_i(\mathcal{M}_B)$ and for all $|\phi\rangle, |\psi\rangle \in \mathcal{K}_1$ and $y \in \mathcal{M}_B$

$$\langle \phi \, | V^* x V \pi_1(y) \psi \, \rangle = \langle \phi \, | V^* x \pi_2(y) V \psi \, \rangle = \langle \phi \, | V^* \pi_2(y) x V \psi \, \rangle = \langle \phi \, | \pi_1(y) V^* x V \psi \, \rangle \ .$$

It follows from (11) that $\omega^1_{A_1C_1} \leq \tau_{A_1} \otimes \sigma_{C_1}$ implies $\omega^2_{A_2C_2} \leq V^*(\tau_{A_1} \otimes \sigma_{C_1})V$ with $V^*(\tau_{A_1} \otimes \sigma_{C_1})V(x) = \tau_{A_1} \otimes \sigma_{C_1}(V^*xV)$. But since V commutes with $\pi_2(\mathcal{M}_A)$, it is of the form $V_A \otimes V_C$ such that $V^*(\tau_A \otimes \sigma_{C_1})V = V_A^* \tau_{A_1} V_A \otimes V_B^* \sigma_{C_1} V_B$. With $\tilde{V}^* \sigma_{C_1} V(\mathbb{1}) \leq \sigma_{C_1}(\mathbb{1})$ and $V_A^* \tau_{A_1} V_A \leq \tau_{A_2}$ we can conclude that $\mathrm{H}_{\min}\left(A_1|C_1\right)_{\omega^1} \leq \mathrm{H}_{\min}\left(A_2|C_2\right)_{\omega^2}$. Since this argument is symmetric, we get equality. □

Note that the duality relation (9) does not conserve classical subsystems. In particular, if we consider a cq-state ω_{XB} where the classical system X is thought of as the subalgebra of diagonal matrices in $M_{|X|}$, then the reduced state of a purification ω_{XBC} of ω_{XB} on $M_{|X|} \otimes \mathcal{M}_C$ is in general not a cq-state anymore.

An operationally more meaningful form for the conditional min- and max-entropy is derived in Section 5. Furthermore, we show some properties of conditional min- and max-entropies at the end of the next section directly for the more general smooth conditional min- and max-entropies.

4.2. **Smooth Min- and Max-Entropies.** Smooth entropies are obtained by optimizing the 'non-smooth' entropies over nearby states. This includes the definition of a suitable distance measure on the set of states. The choice of this measure influences the properties of the smooth entropies crucially. Here we follow [90] and extend the 'purified distance' introduced therein, to the setting of von Neumann algebras.

Distance Measures for Subnormalized States. Let $\mathcal{M}$ be a von Neumann algebra, and $\omega, \sigma \in \mathcal{S}_\leq(\mathcal{M})$. We define the fidelity in accordance with [95] as

$$F_{\mathcal{M}}(\omega, \sigma) = \sup_\pi |\, \langle \xi^\pi_\omega \, | \xi^\pi_\sigma \, \rangle|^2, \tag{12}$$

where the supremum runs over all representations π of $\mathcal{M}$ for which, simultaneously, purifications $|\xi^\pi_\omega\rangle$ and $|\xi^\pi_\sigma\rangle$ of ω and σ exists. The subscript $\mathcal{M}$ denoting the von Neumann algebra will be suppressed if it is clear from the context. Furthermore, if $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$ and ω a pure state state on $\mathcal{M}$ represented by $|\xi_\omega\rangle \in \mathcal{H}$, we define $F_{\mathcal{M}}(|\xi_\omega\rangle, \sigma) = F_{\mathcal{M}}(\omega, \sigma)$. If one chooses a particular representation π on $\mathcal{H}$ in which ω, σ can be represented as vector states, and one takes arbitrary representatives $|\xi_\omega\rangle, |\xi_\sigma\rangle \in \mathcal{H}$ of them, the fidelity can be expressed as [1]

$$F(\omega, \sigma) = \sup_{U \in \pi(\mathcal{M})'} |\, \langle \xi_\omega \, | U \xi_\sigma \, \rangle|^2 \ , \tag{13}$$

where the supremum is taken over unitaries U in $\pi(\mathcal{M})'$. Since the optimization can be extended over the σ-weakly compact set of all U with $\|U\| \leq 1$, and the map $U \mapsto \langle \xi_\omega, U \xi_\sigma \rangle$ is σ-weakly

continuous, we know that the supremum is attained. Note that the optimization over all unitaries in the commutant is equivalent to the optimization over all possible purifications of σ in $\mathcal{H}$. From this it follows that $F_{\mathcal{B}(\mathcal{H})}(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|^2$ for all $|\psi\rangle, |\phi\rangle \in \mathcal{H}$. Another important property of the fidelity is that it can only increase under a quantum channel $\mathcal{E}$ [1]

$$F(\omega, \sigma) \leq F(\mathcal{E}(\omega), \mathcal{E}(\sigma)) \ . \tag{14}$$

As a special case of this inequality we find that $F_{\mathcal{M}}(\omega, \sigma) \geq F_{\mathcal{N}}(\omega, \sigma)$ for $\mathcal{N} \subset \mathcal{M}$.

The fidelity can be used to define distance measures on the set of normalized states [19, 41]. We generalize the fidelity in the same way as it was done in the finite-dimensional case [90], such that it serves as the base of a distance measure on the set of subnormalized states. For that, we first introduce the concept of a projective embedding. Let $\mathcal{M}, \mathcal{N}$ be a von Neumann algebras. Then we say that $\mathcal{N}$ admits a projective embedding of $\mathcal{M}$, denoted by $\mathcal{M} \curvearrowright \mathcal{N}$, if there exists a projector p in $\mathcal{N}$ such that $p\mathcal{N}p$ is isomorphic to $\mathcal{M}$.[15] Note that this is equivalent to the existence of a projector p in $\mathcal{N}$ and a faithful representation π of $\mathcal{M}$ into $\mathcal{N}$ such that $\pi(\mathcal{M}) = (\mathbb{1} - p) \oplus p\mathcal{N}p$. This concept allows us to interpret subnormalized states as the result of an incomplete measurement. In particular, given $\omega \in \mathcal{S}_{\leq}(\mathcal{M})$ and $\mathcal{M} \curvearrowright \mathcal{N}$ with $\mathcal{M} \cong p\mathcal{N}p$, there exists an extended state $\bar{\omega} \in \mathcal{S}(\mathcal{N})$ such that $\bar{\omega}(pxp) = \omega(x)$ for $x \in \mathcal{N}$, where we identified $\mathcal{M}$ and $p\mathcal{N}p$.[16] We then interpret each measurement in $\mathcal{M}$ as incomplete and complete it by adding the no event $(\mathbb{1} - p)$, which leads to the same results as considering the state ω on $\mathcal{M}$. Based on the concept of a projecting embedding, the generalized fidelity is defined similarly as in the finite-dimensional case [90].

Definition 4.5. *Let $\mathcal{M}$ be a von Neumann algebra, and $\omega, \sigma \in \mathcal{S}_{\leq}(\mathcal{M})$. The generalized fidelity between σ and ω is defined as*

$$\mathcal{F}_{\mathcal{M}}(\omega, \sigma) = \sup_{\mathcal{M} \curvearrowright \mathcal{N}} \sup_{\bar{\omega}, \bar{\sigma} \in \mathcal{S}(\mathcal{N})} F_{\mathcal{N}}(\bar{\sigma}, \bar{\omega}) \ , \tag{15}$$

where the second supremum runs over all extended normalized states on $\mathcal{N}$ such that $\bar{\omega}(p \cdot p)$ on $p\mathcal{N}p \cong \mathcal{M}$ corresponds to ω and similarly for $\bar{\sigma}$.

Due to $\mathcal{M} \curvearrowright \mathcal{M} \oplus \mathbb{C}$, the generalized fidelity can be simplified as follows [90].

Lemma 4.6. *Let $\mathcal{M}$ be a von Neumann algebra, and $\omega, \sigma \in \mathcal{S}_{\leq}(\mathcal{M})$. Then*

$$\mathcal{F}_{\mathcal{M}}(\omega, \sigma)^{\frac{1}{2}} = F_{\hat{\mathcal{M}}}(\hat{\omega}, \hat{\sigma})^{\frac{1}{2}} = F_{\mathcal{M}}(\omega, \sigma)^{\frac{1}{2}} + (1 - \omega(\mathbb{1}))^{\frac{1}{2}}(1 - \sigma(\mathbb{1}))^{\frac{1}{2}} \ , \tag{16}$$

where $\hat{\mathcal{M}} = \mathcal{M} \oplus \mathbb{C}$, $\hat{\omega} = \omega \oplus (1 - \omega(\mathbb{1}))$ and $\hat{\sigma} = \sigma \oplus (1 - \sigma(\mathbb{1}))$.

Proof. The proof is conceptually the same as in [90, Lemma 3]. Let $\mathcal{N}$ be such that $\mathcal{M} \curvearrowright \mathcal{N}$ with p the corresponding projector such that $\mathcal{M} \cong p\mathcal{N}p$. Furthermore let $\bar{\omega}, \bar{\sigma}$ be extensions of ω, σ on $\mathcal{N}$ satisfying the required properties. According to the definition of the fidelity we have that $F_{\mathcal{N}}(\bar{\omega}, \bar{\sigma}) = \sup |\langle \xi_{\bar{\omega}}^{\pi} | \xi_{\bar{\sigma}}^{\pi} \rangle|^2$, where the supremum runs over all representations admitting a purification of $\bar{\omega}, \bar{\sigma}$. Now note that all such representations π are also representations of $\mathcal{M}$, that $\xi_{\omega}^{\pi} = \pi(p)\xi_{\bar{\omega}}^{\pi}$ is a purification of ω, and that the same also holds for $\xi_{\sigma}^{\pi} = \pi(p)\xi_{\bar{\sigma}}^{\pi}$. We can then use the Cauchy-Schwarz inequality to compute

$$\begin{aligned} |\langle \xi_{\bar{\omega}}^{\pi} | \xi_{\bar{\sigma}}^{\pi} \rangle| &= |\langle \xi_{\omega}^{\pi} | \xi_{\sigma}^{\pi} \rangle| + |\langle (\mathbb{1} - p)\xi_{\bar{\omega}}^{\pi} | (\mathbb{1} - p)\xi_{\bar{\sigma}}^{\pi} \rangle| \leq |\langle \xi_{\omega}^{\pi} | \xi_{\sigma}^{\pi} \rangle| + \sqrt{\|(\mathbb{1} - p)\xi_{\bar{\omega}}^{\pi}\| \|(\mathbb{1} - p)\xi_{\bar{\sigma}}^{\pi}\|} \\ &\leq |\langle \xi_{\omega}^{\pi} | \xi_{\sigma}^{\pi} \rangle| + \sqrt{(1 - \omega(\mathbb{1}))(1 - \sigma(\mathbb{1}))} \ . \end{aligned}$$

Since this holds for all π, we have that $\mathcal{F}_{\mathcal{N}}(\bar{\omega}, \bar{\sigma})^{\frac{1}{2}} \leq F_{\mathcal{M}}(\omega, \sigma)^{\frac{1}{2}} + (1 - \omega(\mathbb{1}))^{\frac{1}{2}}(1 - \sigma(\mathbb{1}))^{\frac{1}{2}}$ for all $\mathcal{N}$ such that $\mathcal{M} \curvearrowright \mathcal{N}$ and all suitable $\bar{\omega}, \bar{\sigma}$ on $\mathcal{N}$. Hence, we get

$$\mathcal{F}_{\mathcal{M}}(\omega, \sigma)^{\frac{1}{2}} \leq F_{\mathcal{M}}(\omega, \sigma)^{\frac{1}{2}} + (1 - \omega(\mathbb{1}))^{\frac{1}{2}}(1 - \sigma(\mathbb{1}))^{\frac{1}{2}} \ .$$

Finally it is easy to check that the specific choice $\hat{\mathcal{M}}$ together with $\hat{\omega}$ and $\hat{\sigma}$ achieves equality. □

[15] Note that if $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$ and $V : \mathcal{H} \to \mathcal{H}'$ is an isometry, it follows that $\mathcal{M} \curvearrowright \mathcal{B}(\mathcal{H}')$ with the projector $p = VV^*$ [90].

[16] Choose for instance $\bar{\omega}(x) = \omega(pxp) + \sigma((\mathbb{1} - p)x(\mathbb{1} - p))$ with $\sigma \in \mathcal{S}_{\leq}(\mathcal{N})$ such that $\sigma(\mathbb{1} - p) = 1 - \omega(p)$.

The purified distance is then defined as in the finite-dimensional case [90].

Definition 4.7. *Let $\mathcal{M}$ be a von Neumann algebra, and $\omega, \sigma \in \mathcal{S}_{\leq}(\mathcal{M})$. The purified distance between ω and σ is defined as*[17]

$$\mathcal{P}_{\mathcal{M}}(\omega, \sigma) = \sqrt{1 - \mathcal{F}_{\mathcal{M}}(\omega, \sigma)} \ . \tag{17}$$

Like for the fidelity, we omit the indication of the von Neumann algebra for $\mathcal{P}$ whenever it is clear from the context, and write $\mathcal{P}_{\mathcal{M}}(\omega, \sigma) = \mathcal{P}_{\mathcal{M}}(|\xi\rangle, \sigma)$ if $|\xi\rangle$ is a purification of ω. For $\mathcal{P}(\omega, \sigma) \leq \epsilon$ we also use the notation $\omega \approx_\epsilon \sigma$, and say that ω and σ are ϵ-close. A detailed discussion of the properties of the purified distance can be found in [90]. Although their scope is restricted to finite-dimensional Hilbert spaces, many of the properties follow in the same way for general systems described by von Neumann algebras. It is for instance easy to see that the purified distance defines a metric on $\mathcal{S}_{\leq}(\mathcal{M})$. The following Lemma shows the equivalence to the norm distance on $\mathcal{N}(\mathcal{M})$.

Lemma 4.8. *Let $\mathcal{M}$ be a von Neumann algebra, and $\omega, \sigma \in \mathcal{S}_{\leq}(\mathcal{M})$. Then*

$$\sqrt{\|\omega - \sigma\| + |\omega(\mathbb{1}) - \sigma(\mathbb{1})|} \geq \mathcal{P}_{\mathcal{M}}(\sigma, \omega) \geq \frac{1}{2}\big(\|\omega - \sigma\| + |\omega(\mathbb{1}) - \sigma(\mathbb{1})|\big) \ . \tag{18}$$

Proof. The proof can be stated in the same way as in [90] based on the relation

$$1 - \sqrt{F(\omega, \sigma)} \leq \frac{1}{2}\|\omega - \sigma\| \leq \sqrt{1 - F(\omega, \sigma)} \ ,$$

where the first inequality was shown in [19] and the second one in [95]. □

It is important that the purified distance is defined in such a way that it is monotone under completely positive, unital contractions.

Lemma 4.9. *Let $\mathcal{M}$ be a von Neumann algebra, $\omega, \sigma \in \mathcal{S}_{\leq}(\mathcal{M})$, and $\mathcal{E}$ completely positive, unital contraction. Then*

$$\mathcal{P}(\omega, \sigma) \geq \mathcal{P}(\mathcal{E}(\omega), \mathcal{E}(\sigma)) \ . \tag{19}$$

Proof. The finite dimensional version of this is [90, Lemma 7]. The lemma is a direct consequence of the definition of the generalized fidelity and equation (14), from which it follows that $\mathcal{F}(\omega, \sigma) \leq \mathcal{F}(\mathcal{E}(\omega), \mathcal{E}(\sigma))$. □

Definition of Smooth Min- and Max-Entropies. The smoothing set around $\omega \in \mathcal{S}_{\leq}(\mathcal{M})$ is defined as an ϵ-ball in the topology induced by the purified distance.

Definition 4.10. *Let $\mathcal{M}$ be a von Neumann algebra, $\omega \in \mathcal{S}_{\leq}(\mathcal{M})$, and $\epsilon \geq 0$. We define*

$$\mathcal{B}^\epsilon_{\mathcal{M}}(\omega) = \{\sigma \in \mathcal{S}_{\leq}(\mathcal{M}) : \mathcal{P}_{\mathcal{M}}(\omega, \sigma) \leq \epsilon\} \ . \tag{20}$$

We usually omit the indication of the von Neumann algebra in the subscript of the smoothing set if it is clear from the context.

Definition 4.11. *Let $\mathcal{M}_{AB} = M_n \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra, $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$ and $\epsilon \geq 0$. The ϵ-smooth min-entropy of ω_{AB} conditioned on B is defined as*

$$\mathrm{H}^\epsilon_{\min}(A|B)_\omega = \sup_{\bar{\omega}_{AB} \in \mathcal{B}^\epsilon(\omega_{AB})} \mathrm{H}_{\min}(A|B)_{\bar{\omega}} \ , \tag{21}$$

and the ϵ-smooth max-entropy of ω_{AB} conditioned on B as

$$\mathrm{H}^\epsilon_{\max}(A|B)_\omega = \inf_{\bar{\omega}_{AB} \in \mathcal{B}^\epsilon(\omega_{AB})} \mathrm{H}_{\max}(A|B)_{\bar{\omega}} \ . \tag{22}$$

[17] The name purified distance comes from the finite-dimensional case, where the purified distance between two states corresponds to the minimal l_1-distance between purifications of these states. It is straightforward to see that the same result also holds in the von Neumann case, namely, $\mathcal{P}_{\mathcal{M}}(\omega, \sigma) = \frac{1}{2} \inf_\pi \| |\xi^\pi_\omega\rangle\langle\xi^\pi_\omega| - |\xi^\pi_\sigma\rangle\langle\xi^\pi_\sigma| \|_1$, where the infimum runs over all representations of $\mathcal{M}$ in which ω and σ have a vector representation denoted by $|\xi^\pi_\omega\rangle$ and $|\xi^\pi_\sigma\rangle$, respectively.

Note that for $\epsilon = 0$, we retrieve the conditional min- and max-entropy, respectively. This is due to the fact that the purified distance defines a metric on $\mathcal{S}_{\leq}(\mathcal{M}_{AB})$. Furthermore, if the A system is a classical system X, the optimization for the smooth conditional min- and max-entropy of a cq-state $\omega_{XB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$ can, without loss of generality, be restricted to cq-states in $\mathcal{B}^{\epsilon}_{M_{|X|}}(\omega_{XB})$.

Lemma 4.12. *Let $\mathcal{M}_B$ be a von Neumann algebras, X be a set of finite cardinality $|X|$, and $\omega_{XB} \in \mathcal{S}_{\leq}(\ell^{\infty}(X) \otimes \mathcal{M}_B)$. Then*

$$\mathrm{H}^{\epsilon}_{\min}(X|B)_{\omega} = \sup_{\bar{\omega}_{XB} \in \mathcal{B}^{\epsilon}_{\mathrm{cq}}(\omega_{XB})} \mathrm{H}_{\min}(X|B)_{\bar{\omega}}$$
$$\mathrm{H}^{\epsilon}_{\max}(X|B)_{\omega} = \inf_{\bar{\omega}_{XB} \in \mathcal{B}^{\epsilon}_{\mathrm{cq}}(\omega_{XB})} \mathrm{H}_{\max}(X|B)_{\bar{\omega}} \ ,$$

where $\mathcal{B}^{\epsilon}_{\mathrm{cq}}(\omega_{XB}) := \{\sigma_{XB} \in \mathcal{S}_{\leq}(\ell^{\infty}(X) \otimes \mathcal{M}_B) \ : \ \mathcal{P}(\omega_{XB}, \sigma_{XB}) \leq \epsilon\}$.

Proof. The proof can be carried over from the finite-dimensional case, discussed in [72, Remark 3.2.4] for the min-entropy, and in [70, Lemma 3] for the max-entropy. For the sake of completeness we sketch the idea. In the following let $\bar{\omega}_{XB} \in \mathcal{B}^{\epsilon}_{M_{|X|} \otimes \mathcal{M}_B}(\omega_{XB})$. Let $\mathcal{E} : \ell^{\infty}(X) \to M_{|X|}$ be the quantum channel which projects onto the classical basis of X. It follows from equation (19) that $\mathcal{E} \otimes \mathrm{id}(\bar{\omega}_{XB}) \in \mathcal{B}^{\epsilon}_{\mathrm{cq}}(\omega_{XB})$, and a straightforward calculation shows that $\mathrm{H}_{\min}(X|B)_{\bar{\omega}} \leq \mathrm{H}_{\min}(X|B)_{\mathcal{E} \otimes \mathrm{id}(\bar{\omega})}$. This proves the part for the min-entropy. For the max-entropy we take a purification $\{|\xi\rangle, \pi, \mathcal{H}\}$ of $\bar{\omega}_{XB}$ on a Hilbert space $\mathcal{H} = \mathbb{C}^{|X|} \otimes \mathbb{C}^{|X|} \otimes \mathcal{H}_B$, where $\mathcal{M}_B$ acts on $\mathcal{H}_B$ and the complementary system of $\mathcal{M}_{XB}$ is given by $\mathcal{M}_{X'C} = M_{|X|} \otimes \pi(\mathcal{M}_B)$. By the duality between the min- and max-entropy the problem passes over to show that $\mathrm{H}_{\min}(X|X'C)_{\bar{\omega}} \leq \mathrm{H}_{\min}(X|X'C)_{\mathcal{E}_{XX'} \otimes \mathrm{id}(\bar{\omega})}$ for $\mathcal{E}_{XX'}$ the projection onto the subspace given by $P^{XX'} = \sum_{x \in X} |x\rangle\langle x| \otimes |x\rangle\langle x|$, while the cq-state given by the restriction of $\mathcal{E}_{XX'} \otimes \mathrm{id}(\bar{\omega}_{XBC})$ onto $\mathcal{M}_{XB}$ is still in $\mathcal{B}^{\epsilon}_{M_{|X|} \otimes \mathcal{M}_B}(\omega_{XB})$. But this follows in complete analogy to [70, Lemma 3]. □

The ball $\mathcal{B}^{\epsilon}_{\mathcal{M}}(\cdot)$ is chosen in such a way that the smooth conditional min-entropy is unaffected by freedoms which could potentially come from the non-uniqueness of purifications. This can be seen as the smooth analogue of Lemma 4.4, and is connected to the fact that the smooth min-entropy is independent under a projecetive embedding of the physical system into a larger one.

Lemma 4.13. *Let $\mathcal{M}_{AB}$ be a bipartite von Neumann algebra, $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$, $(\pi_i, \mathcal{K}_i, |\xi_i\rangle)$ with $i = 1, 2$ two purifications of ω_{AB} with $\mathcal{M}_{A_i} = \pi_i(\mathcal{M}_A)$ and complementary systems $\mathcal{M}_{C_i}$, and $\epsilon \geq 0$. Then*

$$\mathrm{H}^{\epsilon}_{\min}(A_1|C_1)_{\omega^1} = \mathrm{H}^{\epsilon}_{\min}(A_2|C_2)_{\omega^2} \ , \tag{23}$$

where $\omega^i_{A_iC_i}$ is the restricted state corresponding to $|\xi_i\rangle$.

Proof. The ideas for the proof are adapted from [90]. First, we observe that due to the symmetry of equation (23) it is enough to show inequality in one direction. According to Lemma 3.4, we know that there exists a partial isometry $V : \mathcal{K}_1 \to \mathcal{K}_2$ with $|\xi_2\rangle = V|\xi_1\rangle$ and $V\pi_1(a) = \pi_2(a)V$ for all $a \in \mathcal{M}_{AB}$. Furthermore, we know from the proof of Lemma 4.4 that for all $\sigma_{A_1C_1} \in \mathcal{S}_{\leq}(\mathcal{M}_{A_1C_1})$ the subnormalized state $V^*\sigma_{A_1C_1}V(x) = \sigma_{A_1C_1}(V^*xV)$ on $\mathcal{M}_{A_2C_2}$ satisfies $\mathrm{H}_{\min}(A_1|C_1)_{\sigma} \leq \mathrm{H}_{\min}(A_2|C_2)_{V^*\sigma V}$ and $V^*\omega^1_{A_1C_1}V = \omega^2_{A_2C_2}$. Hence,

$$\mathrm{H}^{\epsilon}_{\min}(A_1|C_1)_{\omega^1} = \sup_{\sigma_{A_1C_1} \in \mathcal{B}^{\epsilon}(\omega^1_{A_1C_1})} \mathrm{H}_{\min}(A_1|C_1)_{\omega} \leq \sup_{\sigma_{A_1C_1} \in \mathcal{B}^{\epsilon}(\omega^1_{A_1C_1})} \mathrm{H}_{\min}(A_2|C_2)_{V^*\sigma V} \ ,$$

and the only thing which is left to prove is that $V^*\sigma_{A_1C_1}V \in \mathcal{B}^{\epsilon}(\omega^2_{A_2C_2})$ for all $\sigma_{A_1C_1} \in \mathcal{B}^{\epsilon}(\omega^1_{A_1C_1})$. But this is equivalent to show that $\mathcal{F}(\omega_{A_1C_1}, \sigma_{A_1C_1}) \leq \mathcal{F}(V^*\omega_{A_1C_1}V, V^*\sigma_{A_1C_1}V)$. Let $p = VV^*$ be the projector onto the image of V. Since $p\mathcal{M}_{A_2C_2}p$ is a von Neumann algebra and $V^*\omega_{A_1C_1}V, V^*\sigma_{A_1C_1}V$ have support projection p, we can use Definition 4.5 to compute

$$\mathcal{F}_{\mathcal{M}_{A_2C_2}}(V^*\omega_{A_1C_1}V, V^*\sigma_{A_1C_1}V) = \mathcal{F}_{p\mathcal{M}_{A_2C_2}p}(V^*\omega_{A_1C_1}V, V^*\sigma_{A_1C_1}V) = \sup_{p\mathcal{M}_{A_2C_2}p \hookrightarrow \hat{\mathcal{N}}} \sup_{\bar{\omega},\bar{\sigma}} F_{\mathcal{N}}(\bar{\omega}, \bar{\sigma})$$
$$\geq F_{\hat{\mathcal{M}}_{A_1C_1}}(\hat{\omega}^1_{A_1C_1}, \hat{\sigma}_{A_1C_1}) = \mathcal{F}_{\mathcal{M}_{A_1C_1}}(\omega^1_{A_1C_1}, \sigma_{A_1C_1}) \ ,$$

where $\hat{\mathcal{M}}_{A_1C_1}, \hat{\omega}^1_{A_1C_1}, \hat{\sigma}_{A_1C_1}$ are like in Lemma 4.6, and the inequality follows from $p\mathcal{M}_{A_2C_2}p \curvearrowright \hat{\mathcal{M}}_{A_1C_1}$ via the isometry $V \oplus 1$, and $\hat{\omega}^1_{A_1C_1}, \hat{\sigma}_{A_1C_1}$ are extensions of $V^*\omega_{A_1C_1}V, V^*\sigma_{A_1C_1}V$ in accordance with (15). □

Next we show that the duality relation also holds for the smooth min- and max-entropies.

Proposition 4.14. *Let $\mathcal{M}_{AB}$ be a bipartite von Neumann algebra, $\omega_{AB} \in \mathcal{S}_\leq(\mathcal{M}_{AB})$, $(\pi, \mathcal{K}, |\xi\rangle)$ an arbitrary purification of ω_{AB} with complementary system $\mathcal{M}_C = \pi(\mathcal{M}_{AB})'$, and $\epsilon \geq 0$. Then*

$$\mathrm{H}^\epsilon_{\max}(A|B)_\omega = -\mathrm{H}^\epsilon_{\min}(A|C)_\omega \ . \tag{24}$$

Proof. The ideas for the proof are adapted from [90]. Because of Lemma 4.13 we can assume that π together with $\mathcal{K}$ is a standard form of $\mathcal{M}$ (see Definition A.2) such that each state in $\mathcal{M}_{AB}$ admits a purification in $\mathcal{K}$. According to the definitions of the smooth entropies we therefore have to show that

$$\sup_{\sigma_{AB} \in \mathcal{B}^\epsilon(\omega_{AB})} \mathrm{H}_{\min}(A|C)_{|\xi_\sigma\rangle} = \sup_{\eta_{AC} \in \mathcal{B}^\epsilon(\omega_{AC})} \mathrm{H}_{\min}(A|C)_\eta \ , \tag{25}$$

where $|\xi_\sigma\rangle \in \mathcal{K}$ is a purification of σ_{AB}. From Lemma 4.4, we know that the min-entropy does not depend on the particular choice of the purification $|\xi_\sigma\rangle$. We can therefore choose $|\xi_\sigma\rangle$ such that $\mathcal{F}_{\mathcal{M}_{AB}}(\omega_{AB}, \sigma_{AB}) = \mathcal{F}_{\mathcal{B}(\mathcal{H})}(\xi, \xi_\sigma)$, and thus,

$$\mathcal{P}_{\mathcal{M}_{AB}}(\omega_{AB}, \sigma_{AB}) = \mathcal{P}_{\mathcal{B}(\mathcal{H})}(|\xi\rangle, |\xi_\sigma\rangle) \geq \mathcal{P}_{\mathcal{M}_{AC}}(|\xi\rangle, |\xi_\sigma\rangle) \ ,$$

from which '$\leq$' in (25) follows. In order to proof the opposite direction we observe that there exists a von Neumann algebra $\mathcal{N} \subset \mathcal{B}(\tilde{\mathcal{K}})$ such that $\mathcal{M}_{ABC} \curvearrowright \mathcal{N}$ and each state η_{AC} has a purification ξ_η in $\tilde{\mathcal{K}}$.[18] Let p be the projector such that $\mathcal{M}_{ABC}$ is isomorphic to $p\mathcal{N}p$ and identify $p\tilde{\mathcal{K}}$ with $\mathcal{K}$. Hence, we can find a purification $|\xi\rangle$ of ω_{AB} in $\tilde{\mathcal{K}}$ with $p|\xi\rangle = |\xi\rangle$. Moreover, we know that for all η_{AC} exists a $|\xi_\eta\rangle \in \tilde{\mathcal{K}}$ with $\mathcal{P}_{\mathcal{M}_{AC}}(\eta_{AC}, \omega_{AC}) = \mathcal{P}_{\mathcal{B}(\tilde{\mathcal{K}})}(|\xi\rangle, |\xi_\eta\rangle)$. Thus,

$$\sup_{\eta_{AC} \in \mathcal{B}^\epsilon(\omega_{AC})} \mathrm{H}_{\min}(A|C)_\eta = \sup_{\||\chi\rangle\| \leq 1, \mathcal{P}_{\mathcal{B}(\tilde{\mathcal{K}})}(|\xi\rangle, |\chi\rangle) \leq \epsilon} \mathrm{H}_{\min}(A|C)_{|\chi\rangle} = \sup_{\||\chi\rangle\| \leq 1, \mathcal{P}_{\mathcal{B}(\tilde{\mathcal{K}})}(|\xi\rangle, |\chi\rangle) \leq \epsilon} \mathrm{H}_{\min}(A|C)_{p|\chi\rangle} \ ,$$

where the last equality is due to $\mathcal{M}_{ABC} \cong p\mathcal{N}p$, wherefore $|\chi\rangle$ and $p|\chi\rangle$ induce the same states on $\mathcal{M}_{ABC}$. Since $\mathcal{P}_{\mathcal{B}(\tilde{\mathcal{K}})}(|\xi\rangle, |\chi\rangle) \geq \mathcal{P}_{\mathcal{M}_{AB}}(|\xi\rangle, |\chi\rangle)$ and each η_{AB} admits a purification in $\mathcal{K}$, we find '$\geq$' in (25). □

4.3. **Elementary Properties of Smooth Entropies.** The smooth conditional min- and max-entropy exhibit some nice entropic behaviors. An important one being that local operations on the system B can never decrease the uncertainty about the system A. This is called the data processing inequality, and is shown for the finite-dimensional case in [90].

Proposition 4.15. *Let $\mathcal{M}_{AB} = M_n \otimes \mathcal{M}_B$ and $\mathcal{M}_C$ be von Neumann algebras, $\omega_{AB} \in \mathcal{S}_\leq(\mathcal{M}_{AB})$, $\mathcal{E} : \mathcal{M}_C \to \mathcal{M}_B$ a quantum channel, and $\epsilon \geq 0$. Then*

$$\mathrm{H}^\epsilon_{\min}(A|B)_\omega \leq \mathrm{H}^\epsilon_{\min}(A|C)_{\mathrm{id}_A \otimes \mathcal{E}_*(\omega)} \tag{26}$$

$$\mathrm{H}^\epsilon_{\max}(A|B)_\omega \leq \mathrm{H}^\epsilon_{\max}(A|C)_{\mathrm{id}_A \otimes \mathcal{E}_*(\omega)} \ . \tag{27}$$

Proof. The ideas of the proof are adapted from [90, Theorem 18]. We first consider the case for the conditional min-entropy for $\epsilon = 0$. Because $\mathcal{E}$ is completely positive, we have that $\omega_{AB} \leq \tau_A \otimes \sigma_B$ implies $\mathrm{id}_A \otimes \mathcal{E}_*(\omega_{AB}) \leq \tau_A \otimes \mathcal{E}_*(\sigma_B)$. Furthermore, since $\mathcal{E}$ is unital, we find that $\mathcal{E}_*(\sigma_B) \in \mathcal{S}(\mathcal{M}_C)$ whenever $\sigma_B \in \mathcal{S}(\mathcal{M}_C)$. Together with the definition of the conditional min-entropy, the inequality follows. For $\epsilon > 0$, the inequality follows straightforwardly by using the fact that the purified distance is monotonically decreasing under quantum channels (19). Now we lift the property from the smooth conditional min- to the smooth conditional max-entropy via the duality. For that we take a purification $(\mathcal{H}, \pi, |\xi\rangle)$ of ω_{AB} on $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_B$ with $\mathcal{H}_A = \mathcal{H}_{A'} = \mathbb{C}^n$ such that

[18] We can choose the standard form to be $\mathcal{K} = \mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathcal{H}^\phi_B$ with $\mathcal{H}^\phi_B$, $\mathcal{M}^\phi_B$ a standard form of $\mathcal{M}_B$. We then have that the complementary system is $\mathcal{M}_C = \mathbb{C}^n \otimes (\mathcal{M}^\phi_B)'$. Hence we can choose $\tilde{\mathcal{K}} = \mathbb{C}^{n^4} \otimes \mathcal{H}^\phi_B$ and $\mathcal{N} = M_{n^4} \otimes \mathcal{M}^\phi_B \vee (\mathcal{M}^\phi_B)'$.

$\pi(\mathcal{M}_A) = \mathcal{B}(\mathcal{H}_A)$ and $\pi(\mathcal{M}_B) \subset \mathcal{B}(\mathcal{H}_B)$. We remark that the concatenation $\hat{\mathcal{E}} = \pi \circ \mathcal{E}$ is a completely positive, unital map from $\mathcal{M}_C$ onto $\pi(\mathcal{M}_B)$. Due to Stinespring's dilation theorem [62] there exists a Hilbert space $\mathcal{H}_C = \mathcal{H}_R \oplus \mathcal{H}_B$, a representation $\pi_{\mathcal{E}}$ of $\mathcal{M}_C$ on $\mathcal{H}_C$, and an isometry $V : \mathcal{H}_B \to \mathcal{H}_C$ such that $\hat{\mathcal{E}}(a) = V^* \pi_{\mathcal{E}}(a) V$ for all $a \in \mathcal{M}_C$. Hence for all $y \in \mathcal{M}_{AC}$

$$[\mathrm{id}_A \otimes \mathcal{E}_*(\omega_{AB})](y) = \omega_{AB}(\mathrm{id}_A \otimes \mathcal{E}(y)) = \langle \xi \,|(\mathbb{1}_{AA'} \otimes V^*)(\mathrm{id}_A \otimes \pi_{\mathcal{E}})(y)(\mathbb{1}_{AA'} \otimes V)\xi \rangle \ ,$$

wherefore we can conclude that $(\mathcal{H}, \pi_{\mathcal{E}}, \mathbb{1}_{AA'} \otimes V|\xi\rangle)$ is a purification of $\mathrm{id}_A \otimes \mathcal{E}_*(\omega_{AB})$. If we denote $\mathcal{M}_{B'} = \pi(\mathcal{M}_B)'$, $\mathcal{M}_{C'} = \pi_{\mathcal{E}}(\mathcal{M}_C)$ and $\mathcal{M}_{V(C')} = V^* \pi_{\mathcal{E}}(\mathcal{M}_C)' V$, we obtain from $V^* \pi_{\mathcal{E}}(\mathcal{M}_C) V \subset \mathcal{M}_B$ that $\mathcal{M}_{B'} \subset \mathcal{M}_{V(C')}$. Because the map $x \to V^* x V$ from $\mathcal{M}_{C'}$ into $V(\mathcal{M}_{C'})$ is unital and completely positive, the restriction on a subalgebra is a quantum channel and $\mathbb{1} \otimes V^* V|\xi\rangle = |\xi\rangle$, we obtain via the duality

$$\begin{aligned} \mathrm{H}^{\epsilon}_{\max}(A|C)_{\mathrm{id}_A \otimes \mathcal{E}_*(\omega)} &= -\mathrm{H}^{\epsilon}_{\min}\left(A|A'C'\right)_{\mathbb{1} \otimes V|\xi\rangle} \geq \mathrm{H}^{\epsilon}_{\min}\left(A|A'V(C')\right)_{|\xi\rangle} \\ &\geq -\mathrm{H}^{\epsilon}_{\min}\left(A|A'B'\right)_{|\xi\rangle} = \mathrm{H}^{\epsilon}_{\max}(A|B)_{\omega} \ . \end{aligned}$$

□

As a special case of the data processing inequality we get for von Neumann algebras $\mathcal{M}_C \subset \mathcal{M}_B$, that $\mathrm{H}^{\epsilon}_{\min}(A|B)_{\omega} \leq \mathrm{H}^{\epsilon}_{\min}(A|C)_{\omega}$, as well as $\mathrm{H}^{\epsilon}_{\max}(A|B)_{\omega} \leq \mathrm{H}^{\epsilon}_{\max}(A|C)_{\omega}$, where we utilized that the restriction of a state onto a subalgebra, is a quantum channel. Furthermore, we also obtain

$$\mathrm{H}^{\epsilon}_{\min}(A)_{\omega} \geq \mathrm{H}^{\epsilon}_{\min}(A|B)_{\omega} \geq \mathrm{H}^{\epsilon}_{\min}(A|BC)_{\omega} = -\mathrm{H}^{\epsilon}_{\max}(A)_{\omega} \ ,$$

for ω_{ABC} a purification of $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$. Since the system A is assumed to be finite-dimensional, we can conclude that the smooth conditional min-entropy is always finite. The same argument also shows that the smooth conditional max-entropy is always finite.

5. Operational Interpretations of Min- and Max-Entropies

The definition of good entropy measures ultimately boils down to the question of their operational significance. For the non-smooth min- and max-entropies we derive them in Theorem 5.1 and Theorem 5.5, respectively. For an operational interpretation of the smooth min-entropy we refer to Section 7, where we link it to privacy amplification for the special case of cq-states. The smooth conditional max-entropy of cq-states characterizes classical data compression with quantum side information, see Section 8. For more about possible operational interpretations of the smooth conditional min- and max-entropy analogous to the finite-dimensional case, see Section 10.

Min-Entropy. We generalize the operational meaning of the conditional min-entropy known for finite-dimensional [54] and separable [40] Hilbert spaces.

Theorem 5.1. *Let $\mathcal{M}_{AB} = M_n \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra, $\omega_{AB} = (\omega_B^{ij}) \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$, and $|\Phi_{AA'}\rangle = \sum_{i=1}^n |\phi_i\rangle \otimes |\psi_i\rangle$, where $\{|\phi_i\rangle\}$ and $\{|\psi_i\rangle\}$ are orthonormal bases of $\mathbb{C}^n$. Then*[19]

$$2^{-\mathrm{H}_{\min}(A|B)_{\omega}} = \sup_{\mathcal{E}_*} F((\mathrm{id}_A \otimes \mathcal{E}_*)(\omega_{AB}), |\Phi_{AA'}\rangle) \ , \tag{28}$$

where the supremum is taken over all quantum channels $\mathcal{E} : M_n \to \mathcal{M}_B$.

The proof developed in the following is conceptually different to the finite dimensional one in [54], and is based on the theory of ordered vector spaces [64]. In particular, we employ the fact that $\mathrm{H}_{\min}(A|B)_{\omega}$ is an optimization problem over a subcone of $\mathcal{N}^+(\mathcal{M}_{AB})$. For $\omega_{AB} = (\omega_B^{ij}) \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$ we write

$$\begin{aligned} 2^{-\mathrm{H}_{\min}(A|B)_{\omega}} &= \inf_{\sigma_B \in \mathcal{S}(\mathcal{M}_B)} \inf\{\lambda : \lambda \cdot \tau_A \otimes \sigma_B \geq \omega_{AB}\} \\ &= \inf\{\sigma_B(\mathbb{1}) : \tau_A \otimes \sigma_B \geq \omega_{AB},\, \sigma_B \in \mathcal{N}^+(\mathcal{M}_B)\} \\ &= \inf\{f_{\mathbb{1}}(\sigma_{AB}) : \sigma_{AB} \geq \omega_{AB},\, \sigma_{AB} \in E\} \ , \end{aligned}$$

[19] The difference of a square in comparison to [54, 40] is due to the different definition of the fidelity.

where $f_{\mathbb{1}}(\eta_{AB}) = \frac{1}{n}\eta_{AB}(\mathbb{1})$ for $\eta_{AB} \in \mathcal{N}(\mathcal{M}_{AB})$, and $E = \{\tau_A \otimes \eta_B : \eta_B \in \mathcal{N}^h(\mathcal{M}_B)\}$ with $\mathcal{N}^h(\mathcal{M}_B)$ the set of hermitian functionals on $\mathcal{M}_B$. Considering $\mathcal{N}^h(\mathcal{M}_{AB})$ as a vector space, we have that E is a subspace of $\mathcal{N}^h(\mathcal{M}_{AB})$, and that $f_{\mathbb{1}}$ defines a positive functional on $\mathcal{N}^h(\mathcal{M}_{AB})$. The basic ingredient is now the following extension result for functionals in an ordered vector space.

Lemma 5.2. [64, Lemma 2.13] *Let V be an ordered real vector space with a full cone V^+, $E \subset V$ a subspace which majorizes V^+, $w \in V\backslash E$, and $f : E \to \mathbb{R}$ a positive functional on E. Then there exists a positive extension $\tilde{f}$ on V such that*

$$\tilde{f}(w) = u_f(w) := \inf\{f(v) \ : \ v \geq w, \, v \in E\} \ . \tag{29}$$

Moreover, it holds for all positive functionals g on V with $g|_E = f$, that $g(w) \leq u_f(w)$.

If we take $V = \mathcal{N}^h(\mathcal{M}_{AB})$ with the cone of all positive functional $V^+ = \mathcal{N}^+(\mathcal{M}_{AB})$ and E as defined above, then E majorizes V^+. According to the definition of the predual, the set of all positive functionals on V are given by the positive operators in $\mathcal{M}_{AB}$. Hence by applying Lemma 5.2 with $f \equiv f_{\mathbb{1}}$, we find the following proposition.

Proposition 5.3. *Let $\mathcal{M}_{AB} = M_n \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra, and $\omega_{AB} = (\omega_B^{ij}) \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$. Then*

$$2^{-\mathrm{H}_{\min}(A|B)_\omega} = \sup\{\sum_{ij} \omega_B^{ij}(M_{ij}) \ : \ (M_{ij}) \in (M_n(\mathcal{M}_B))^+, \, \sum_i M_{ii} = \mathbb{1}\} \ . \tag{30}$$

Proof. The only thing left to proof is $\sum_i M_{ii} = \mathbb{1}$. But this follows from the fact that the linear functional given by (M_{ij}) restricted to E, has to be $f_{\mathbb{1}}$, and thus $(\tau_A \otimes \sigma_B)((M_{ij})) = \sum_i \sigma_B(M_{ii}) = 1$ for all $\sigma_B \in \mathcal{S}(\mathcal{M}_B)$. Since $(\mathcal{N}(\mathcal{M}_B))^* = \mathcal{M}_B$ this implies $\sum_i M_{ii} = \mathbb{1}$. □

By the help of (30) we can now prove Theorem 5.1.

Proof of Theorem 5.1. First, we show that there exist for each operator $M = (M_{ij}) \in (M_n(\mathcal{M}_B))^+$ with $\sum_i M_{ii} = \mathbb{1}$, a quantum operation $\mathcal{E}_M$ such that

$$F((\mathrm{id}_A \otimes \mathcal{E}_M)(\omega_{AB}), |\Phi_{AA'}\rangle) = \sum_{ij} \omega_B^{ij}(M_{ij}) \ . \tag{31}$$

Then we show the opposite, namely that for each quantum operation $\mathcal{E}$ exists $M^{\mathcal{E}} \in (M_n(\mathcal{M}_B))^+$ with $\sum_i M_{ii}^{\mathcal{E}} = \mathbb{1}$ such that (31) holds. Together with Proposition 5.3 this implies the statement. For $M = (M_{ij}) \in (M_n(\mathcal{M}_B))^+$ with $\sum_i M_{ii} = \mathbb{1}$ we define the map $\mathcal{E}_M$ via $\mathcal{E}_M(\sigma) = (\sigma(M_{ij})^{ij})$ for $\sigma \in \mathcal{N}(\mathcal{M}_B)$. Here, the states are with respect to the fixed basis in $\mathcal{M}_n$ given by $\{|\psi_i\rangle\}$, such that for $A = \sum_{ij} a_{ij}|\psi_i\rangle\langle\psi_i|$, $(\sigma(M_{ij})^{ij})(A) = \sum_{ij} a_{ij}\sigma(M_{ij})$. It is straightforward to check that $\mathcal{E}_M$ is a quantum operation and satisfies (31). For the opposite direction we define for an arbitrary quantum operation $\mathcal{E}$ the operator $M^{\mathcal{E}}$ via $M_{ij}^{\mathcal{E}} = \mathcal{E}^*(|\psi_i\rangle\langle\psi_j|)$. From the fact that $\mathcal{E}^*$ is completely positive and unital, it follows that $M^{\mathcal{E}}$ is positive and $\sum_i M_{ii}^{\mathcal{E}} = \mathbb{1}$. A short computation shows that the relation (31) holds for $\mathcal{E}$ and $\mathcal{M}^{\mathcal{E}}$ as constructed. □

Guessing Probability. The analogue of Proposition 5.3 for cq-states leads to the guessing probability [54]. We start with a cq-state $\omega_{XB} = (\omega_B^x)_{x\in X}$ on $\ell^\infty(X) \otimes \mathcal{M}_B$, where the classical part given by the finite alphabet X is hold by Alice and the quantum part $\mathcal{M}_B$ by Bob. Bob wants to guess the classical variable hold by Alice by applying the optimal measurement on his part. The guessing probability characterizes the probability that Bob's guess is correct. That is,

$$p_{\mathrm{guess}}(X|B)_\omega = \sup\{\sum_{x\in X} \omega_B^x(E_x) \ : \ E_x \in \mathcal{M}_B, \ E_x \geq 0, \ \sum_x E_x = \mathbb{1}\} \ . \tag{32}$$

Proposition 5.4. *Let $\mathcal{M}_{XB} = \ell^\infty(X) \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ be a von Neumann algebra, and $\omega_{XB} \in \mathcal{S}(\mathcal{M}_{XB})$. Then*

$$\mathrm{H}_{\min}(X|B)_\omega = -\log p_{\mathrm{guess}}(X|B)_\omega \ , \tag{33}$$

with $p_{\mathrm{guess}}(X|B)_\omega$ as defined in (32).

Proof. The proof is a simple application of Lemma 5.2. As in the last section, we write the conditional min-entropy as

$$2^{-\mathrm{H}_{\min}(X|B)_\omega} = \inf\{f_{\mathbb{1}}(\sigma_{XB}) : \sigma_{XB} \geq \omega_{XB},\, \sigma_{XB} \in E\} \ ,$$

where $E = \{e \otimes \sigma_B : \sigma_B \in \mathcal{M}_{B*}\}$ with $e = (1, \ldots, 1)$. Using Lemma 5.2 with $V = \ell^1_{|X|}(\mathcal{M}_B)$ and $V^+ = \ell^1_{|X|}(\mathcal{M}_B)_+$ the assertion follows. □

Max-Entropy. In accordance to the finite-dimensional case [54], we find the following operational meaning of the conditional max-entropy.

Theorem 5.5. *Let $\mathcal{M}_{AB} = M_n \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra, and $\omega_{AB} = (\omega^{ij}_B) \in \mathcal{S}_\leq(\mathcal{M}_{AB})$. Then*

$$2^{\mathrm{H}_{\max}(A|B)_\omega} = \sup_{\sigma_B \in \mathcal{S}(\mathcal{M}_B)} F(\omega_{AB}, \tau_A \otimes \sigma_B) \ , \tag{34}$$

where τ_A denotes the trace on M_n.

Proof. We prove inequality in both directions in a similar way as in the finite-dimensional case [54]. Recall that each state in $\mathcal{M}_{AB}$ can be purified in the standard form, that is, in $M_n \otimes M_n \otimes \mathcal{M}^\phi_B$, where $\mathcal{M}^\phi_B$ is a standard form of $\mathcal{M}_B$. We denote the purifying system by $\mathcal{M}_{A'B'}$ since it consists of a copy of the A-system $\mathcal{M}_{A'} = M_n$ and the commutant $\mathcal{M}_{B'} = (\mathcal{M}^\phi_B)'$ of the system B. Thus, $\mathcal{M}_{ABA'B'} \subset \mathcal{B}(\mathcal{K})$ with $\mathcal{K} = \mathbb{C}^{2n} \otimes \mathcal{H}_\phi$. Let now $\xi_\omega \in \mathcal{K}$ be a purification of ω_{AB} and $|\Phi_{AA'}\rangle$ a non-normalized maximally entangled state on $\mathcal{M}_{AA'}$ as in Corollary 5.1, thus a purification of τ_A. Then with $\eta_\sigma \in \mathcal{H}_\phi$ a purification of $\sigma \in \mathcal{S}(\mathcal{M}_B)$, we find that

$$\begin{aligned} F(\omega_{AB}, \tau_A \otimes \sigma_B) &= \sup_{U \in \mathcal{M}_{A'B'}} |\langle \xi_\omega | U(\Phi_{AA'} \otimes \eta_\sigma) \rangle|^2 = \sup_{U \in \mathcal{M}_{A'B'}} F_{\mathcal{B}(\mathcal{K})}(U\xi_\omega, \Phi_{AA'} \otimes \eta_\sigma) \\ &\leq \sup_{U \in \mathcal{M}_{A'B'}} F_{\mathcal{M}_{AA'}}(U\xi_\omega, \Phi_{AA'} \otimes \eta_\sigma) \ , \end{aligned}$$

where the supremum is taken over unitaries U in $\mathcal{M}_{A'B'}$. According to Stinespring's dilation theorem [62], applying a unitary followed by a restriction of the state is a quantum operation, such that the state on $\mathcal{M}_{AA'}$ described by $U\xi_\omega$ can be obtained by applying a quantum operation $\mathcal{E}_U : \mathcal{N}(\mathcal{M}_{A'B'}) \to \mathcal{N}(M_{A'})$ on $\omega_{AA'B'}$. Hence together with Corollary 5.1

$$F(\omega_{AB}, \tau_A \otimes \sigma_B) \leq \sup_U F_{\mathcal{M}_{AA'}}((\mathrm{id}_A \otimes \mathcal{E}_U)(\omega_{AA'B'}, \Phi_{AA'}) \leq 2^{-\mathrm{H}_{\min}(A|A'B')_\omega} = 2^{\mathrm{H}_{\max}(A|B)_\omega} \ .$$

Taking the supremum over all $\sigma_B \in \mathcal{S}(\mathcal{M}_B)$ we find the inequality in one direction. In order to show the other direction, we note that according to Corollary 5.1, there exists for all $\delta > 0$ a quantum operation $\mathcal{E} : \mathcal{N}(\mathcal{M}_{A'B'}) \to \mathcal{N}(M_{A'})$ such that

$$2^{\mathrm{H}_{\max}(A|B)_\omega} \leq F((\mathrm{id}_A \otimes \mathcal{E})(\omega_{AA'B'}), |\Phi_{AA'}\rangle) + \delta \ . \tag{35}$$

Let now $|\xi_\omega \varepsilon\rangle$ be a purification of $(\mathrm{id}_{AB} \otimes \mathcal{E})(\omega_{ABA'B'})$, which can always be found on the extended system $\mathcal{M}_{AA'CBB'}$, where $\mathcal{M}_C = M_{n^2}$. With an arbitrary $|\theta\rangle \in \mathbb{C}^{n^2} \otimes \mathcal{H}_\phi$, we obtain

$$\begin{aligned} F((\mathrm{id}_A \otimes \mathcal{E})(\omega_{AA'B'}), |\Phi_{AA'}\rangle) &= \sup_{U \in \mathcal{M}_{DBB'}} |\langle \xi_\omega \varepsilon | U(\Phi_{AA'} \otimes \theta) \rangle|^2 \\ &\leq \sup_{U \in \mathcal{M}_{DBB'}} F_{\mathcal{M}_{AB}}(|\xi_\omega \varepsilon\rangle, |\Phi_{AA'}\rangle \otimes |U\theta\rangle) \ . \end{aligned}$$

Since the reduced state of $|\xi_\omega \varepsilon\rangle$ on $\mathcal{M}_{AB}$ is ω_{AB}, and there exists for all $\sigma_B \in \mathcal{S}(\mathcal{M}_B)$ a purification of the form $|U\theta\rangle$ with U unitary in $\mathcal{M}_{DBB'}$, we arrive at

$$2^{\mathrm{H}_{\max}(A|B)_\omega} \leq \sup_{\sigma_B \in \mathcal{S}(\mathcal{M}_B)} F(\omega_{AB}, \tau_A \otimes \sigma_B) + \delta \ . \tag{36}$$

Because this holds for any $\delta > 0$, we found the inequality in the other direction. □

6. Entropic Uncertainty Relations

One of the most fundamental concept in quantum mechanics is the uncertainty principle. It implies that even if one has full classical information about a system, it is impossible to predict the outcomes of all possible measurements. That is, one has an inherent uncertainty about possible measurement outcomes, and since entropies are measures of uncertainty, it is manifest to quantify this uncertainty using entropy measures (see [99, 14] and references therein). Recently it was realized that if one allows to have quantum information about the system in question, the situation qualitatively changes and one has a subtle interplay between uncertainty and entanglement (between the observer and the system). This effect was quantified by entropic uncertainty relations with quantum side information [12, 68, 92, 28, 29]. Note that the scenario is particularly suited to study quantum cryptography, because the adversary might have quantum information as well.

Here we first describe the setup we are interested in, and then state our main theorem; an entropic uncertainty relation with quantum side information (Theorem 6.1), which is a generalization of the finite dimensional result in [92]. The application of this relation to concrete physical systems is ongoing research and will be discussed in a forthcoming paper.

Like in [92] we start with a tripartite quantum state ω_{ABC} and apply a POVM $\{E_A^x\}$ or $\{F_A^y\}$ on system A. We are then interested in the uncertainty system B and system C have about the post-measurement probabilities generated by $\{E_A^x\}$ and $\{F_A^x\}$, respectively, and quantify the uncertainty in terms of the smooth conditional min- and max-entropy. Note that the general von Neumann algebra version of the uncertainty relation given below (Theorem 6.1) can not be proven in this generality by using the techniques of [40].

Theorem 6.1. *Let $\mathcal{M}_{ABC}$ be a tripartite von Neumann algebra, $\omega_{ABC} \in \mathcal{S}(\mathcal{M}_{ABC})$, $\{E_A^x\}$ and $\{F_A^y\}$ POVM's on $\mathcal{M}_A$, and $\epsilon \geq 0$. Then*

$$\mathrm{H}_{\min}^{\epsilon}(X|B)_{\omega} + \mathrm{H}_{\max}^{\epsilon}(Y|C)_{\omega} \geq -\log \max_{x,y} \left\| (E_A^x)^{\frac{1}{2}} \cdot (F_A^y)^{\frac{1}{2}} \right\|^2 , \tag{37}$$

where $\omega_{XB} = (\omega_B^x)$ with $\omega_B^x(\cdot) = \omega_{AB}(E_A^x \cdot)$, and $\omega_{YC} = (\omega_C^y)$ with $\omega_C^y(\cdot) = \omega_{AC}(F_A^y \cdot)$ are cq-states on $\mathcal{M}_B$ and $\mathcal{M}_C$, respectively.

We will derive this theorem from a more general result. But first, we have to introduce some notation. Let $\mathcal{M}_A$ be a von Neumann algebra, and consider a completely positive, unital map $\mathcal{E} : M_n \to \mathcal{M}_A$. As we can always embed $\mathcal{M}_A \subset \mathcal{B}(\mathcal{H})$ faithfully for some $\mathcal{H}$, we can apply Stinespring's dilation theorem to $\mathcal{E}$. Hence there exist a Hilbert space $\mathcal{H}'$, a representation π of M_n on $\mathcal{H}'$ and an isometry $V : \mathcal{H} \to \mathcal{H}'$, such that

$$\mathcal{E}(x) = V^* \, \pi(x) \, V \, .$$

Since M_n is a finite-dimensional algebra, we can choose $\mathcal{H}'$ to be isomorphic to $\mathbb{C}^n \otimes \mathbb{C}^d \otimes \mathcal{H}$ with $1 \leq d \leq n$, and π of the form $\pi(x) = x \otimes \mathbb{1}_d \otimes \mathbb{1}_{\mathcal{H}}$. If $\mathcal{M}_R \subset \mathcal{M}_A'$, is a von Neumann algebra, then we can extend $\mathcal{E}$ to $\tilde{\mathcal{E}} : M_n(\mathcal{M}_R) \to \mathcal{M}_{AR}$ by setting

$$\tilde{\mathcal{E}}\Big(\sum_{ij} x_{ij} \otimes |i\rangle\langle j| \Big) = \sum_{ij} \Big(V^* \, (|i\rangle\langle j| \otimes \mathbb{1}_d \otimes \mathbb{1}_{\mathcal{H}}) V \Big) \, x_{ij}$$

for $\{|i\rangle\}_{i=1}^n$ an orthonormal bases of $\mathbb{C}^n$ and $x_{ij} \in \mathcal{M}_R$. The fact that $\mathcal{M}_R$ is in the commutant of $\mathcal{M}_A$ assures that the map is still completely positive. In the following, we will abbreviate the right hand side of the last equation as $V^* x \otimes \mathbb{1}_d \, V$, for $x \in M_n(\mathcal{M}_R)$. Correspondingly, any map $W : \mathbb{C}^n \otimes \mathbb{C}^d \otimes \mathcal{H} \to \mathbb{C}^n \otimes \mathbb{C}^d \otimes \mathcal{H}$ can be used to define a completely positive map $T_W : M_d \to \mathcal{M}_n(\mathcal{M}_A) \subset \mathcal{B}(\mathbb{C}^n \otimes \mathcal{H})$ via

$$T_W \, : \, |k\rangle\langle l| \mapsto \mathrm{Tr}_d(W^* \, \mathbb{1}_n \otimes |k\rangle\langle l| \otimes \mathbb{1}_{\mathcal{H}} \, W^*) \, .$$

We denote by $c(W)$ the norm of the associated Choi-matrix of this map, that is,

$$c(W) = \Big\| \sum_{k,l} |k\rangle\langle l| \otimes T_W(|k\rangle\langle l|) \Big\|. \tag{38}$$

We are now prepared to state the general theorem from which Theorem 6.1 can be deduced.

Theorem 6.2. *Let $\mathcal{M}_{ABC}$ be a tripartite von Neumann algebra, $\omega_{ABC} \in \mathcal{S}(\mathcal{M}_{ABC})$, $\mathcal{E} : \mathcal{M}_E \to \mathcal{M}_A$ and $\mathcal{G} : \mathcal{M}_G \to \mathcal{M}_A$ completely positive unital maps, their support $\mathcal{M}_E \cong M_{n'}, \mathcal{M}_G \cong M_n$ being matrix algebras, and $\epsilon \geq 0$. If U (resp. V) denote the implementing isometries corresponding to the Stinespring dilation of $\mathcal{E}$ (resp. $\mathcal{G}$), then*

$$\mathrm{H}_{\min}^{\epsilon}(E|B)_{\omega} + \mathrm{H}_{\max}^{\epsilon}(G|C)_{\omega} \geq -\log c(UV^*) \ , \tag{39}$$

where $\omega_{EB}(x) = \omega_{AB}(\tilde{\mathcal{E}}(x))$, $\omega_{GC}(y) = \omega_{AC}(\tilde{\mathcal{G}}(y))$, and $c(.)$ is defined as in (38). Note that the quantity $c(UV^*)$ does not depend on the choice of the particular Stinespring dilations U, V.

Proof. The proof relies on the ideas developed in [92], and can in fact be regarded as the dual version of it. Let $\mathcal{H}$ be a Hilbert space such that $\mathcal{M}_{ABC} \subset \mathcal{B}(\mathcal{H})$ is faithfully embedded and there exist a purifying vector $|\psi\rangle \in \mathcal{H}$ for ω_{ABC}, i.e. $\omega_{ABC}(x) = \langle \psi | x \, \psi \rangle$. We denote by $U : \mathcal{H} \to \mathbb{C}^{n'} \otimes \mathbb{C}^{d'} \otimes \mathcal{H}$ and $V : \mathcal{H} \to \mathbb{C}^{n} \otimes \mathbb{C}^{d} \otimes \mathcal{H}$ the isometries of the Stinespring dilations corresponding to $\mathcal{E}$ and $\mathcal{G}$, respectively, as explained in the discussion preceding the theorem. Due to the fact that $|\psi\rangle$ is a purification of ω_{ABC}, we have that

$$\langle V\psi \, | x \otimes \mathbb{1}_d V\psi \, \rangle = \langle \psi \, | \tilde{\mathcal{G}}(x)\psi \, \rangle = \omega_{ABC}(\tilde{\mathcal{G}}(x)) = \omega_{GC}(x)$$

for $x \in \mathcal{M}_{GC} \cong M_n(\mathcal{M}_B)$, implying that $(\mathrm{id}_{M_n} \otimes \mathbb{1}_d \otimes \mathbb{1}_{\mathcal{H}}, \mathbb{C}^n \otimes \mathbb{C}^d \otimes \mathcal{H}, V|\psi\rangle)$ is a purification of ω_{GC}. Denoting the commutant $\mathcal{M}'_{ABC}$ in $\mathcal{B}(\mathcal{H})$ by $\mathcal{M}_D$, we get that the corresponding complementary system is equal to $M_d(\mathcal{M}_{ABD})$. An analogues argument provides a purification $(\mathrm{id}_{M_{n'}} \otimes \mathbb{1}_{d'} \otimes \mathbb{1}_{\mathcal{H}}, \mathbb{C}^{n'} \otimes \mathbb{C}^{d'} \otimes \mathcal{H}, U|\psi\rangle)$ of ω_{EB} with complementary system $M_{d'}(\mathcal{M}_{ACD})$. Since

$$\mathrm{H}_{\max}^{\epsilon}(G|C)_{\omega} = -\mathrm{H}_{\min}^{\epsilon}(G|dABD)_{V|\psi\rangle}$$

follows from the duality relation of smooth entropies (Proposition 4.14) we have to show that

$$\mathrm{H}_{\min}^{\epsilon}(G|dABD)_{V|\psi\rangle} \leq \mathrm{H}_{\min}^{\epsilon}(E|B)_{U|\psi\rangle} + \log c \ ,$$

where $c = c(UV^*)$ as defined in (38). We first prove the theorem for the case $\epsilon = 0$. By the operational characterization of the conditional min-entropy (Proposition 5.3) the last inequality then amounts to

$$\begin{aligned} \sup\{ \langle \psi \, | U^* x \otimes \mathbb{1}_{d'} \, U\psi \, \rangle \ : x \in M_{n'}(\mathcal{M}_B)^+ , \mathrm{Tr}_{n'}(x) \leq \mathbb{1}_{\mathcal{H}} \} \\ \leq c \cdot \sup\{ \langle \psi \, | V^* \, y \, V\psi \, \rangle \ : \ y \in M_{nd}(\mathcal{M}_{ABD})^+ , \mathrm{Tr}_n(y) \leq \mathbb{1}_{d'} \otimes \mathbb{1}_{\mathcal{H}} \} \ . \end{aligned}$$

Since V^*V projects onto $\mathcal{H}$ and $U|\psi\rangle = UV^*V|\psi\rangle$ the last inequality would follow from

$$\mathrm{Tr}_n(VU^* \, x \otimes \mathbb{1}_{d'} \, UV^*) \ \leq \ c \cdot \mathbb{1}_{d'} \otimes \mathrm{Tr}_{n'}(x) \tag{40}$$

where $x \in M_{n'}(\mathcal{M}_B)$. Expanding into coefficients with respect to an orthonormal basis of $\mathbb{C}^{n,n'} \otimes \mathbb{C}^{d,d'}$, we see that the last inequality is true for c being the norm of the matrix

$$\sum_{m=1}^{d'} \sum_{p=1}^{n} \sum_{i,j=1}^{n'} \sum_{k,l=1}^{d} \langle im \, | UV^* pk \, \rangle \, \langle pl \, | VU^* jm \, \rangle \, |k\rangle\langle l| \otimes |i\rangle\langle j| = \sum_{k,l} |k\rangle\langle l| \otimes T_{UV^*}(|k\rangle\langle l|)$$

as an element in $M_{n'd}(\mathcal{M}_A)$. This concludes the proof for the case $\epsilon = 0$. If now $\epsilon > 0$, take an element $\gamma^{\epsilon}_{GdABD}$ of $\mathcal{B}^{\epsilon}(V|\psi\rangle_{GdABD})$. Here $V|\psi\rangle_{GdABD}$ denotes the vector state $V|\psi\rangle$ restricted to $M_{nd}(\mathcal{M}_{ABD})$. Hence, according to the discussion in Section 4.2, there exist a purifying vector $|\psi^{\epsilon}_V\rangle \in \mathbb{C}^n \otimes \mathbb{C}^d \otimes \mathcal{H}$ of $\gamma^{\epsilon}_{GdABD}$ such that[20]

$$\mathcal{F}(V|\psi\rangle, |\psi^{\epsilon}_V\rangle) \geq 1 - \epsilon^2 \ .$$

[20]This can always be assured by making $\mathcal{H}$ large enough, i.e. by considering the standard form of $\mathcal{M}_{ABC}$.

Again using that $U|\psi\rangle = UV^*V|\psi\rangle$, and the fact that VV^* is a projector, we find

$$\mathcal{F}(U|\psi\rangle, UV^*|\psi_V^\epsilon\rangle) = \mathcal{F}(UV^*V|\psi\rangle, UV^*|\psi^\epsilon\rangle) \geq 1 - \epsilon^2 \ ,$$

implying $UV^*|\psi_V^\epsilon\rangle_{EB} \in \mathcal{B}^\epsilon(U|\psi\rangle_{EB})$. Since the smooth min-entropy is given by the supremum of the min-entropy over all elements in the ϵ-ball, the result follows by repeating the discussion leading to equation (40). □

Remark 6.3. *Since POVM's are special cases of quantum operations, their support being abelian von Neumann algebras, Theorem 6.1 is just a special case of Theorem 6.2. Assume for simplicity that $|X| = |Y| = n$, and think of ℓ_∞^n as the subalgebra of diagonal matrices in M_n. The corresponding isometry for $E : \ell_\infty^n \to \mathcal{M}_A$, $e_x \mapsto E_A^x$, can then be chosen to be of the form*

$$V \ : \ \mathcal{H} \to \mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathcal{H} \ , \quad V|\psi\rangle = \sum_{i=x}^{n} (E_A^x)^{\frac{1}{2}} |\psi\rangle|x\rangle|x\rangle \ ,$$

and analogously for $F : \ell_\infty^n \to \mathcal{M}_A$, $e_x \mapsto F_A^x$. Here $\{e_x\}$ denotes the canonical basis for ℓ_∞^n. Hence we get

$$\begin{aligned} c(UV^*) &= \Big\| \sum_{k,l} |k\rangle\langle l| \otimes T_{UV^*}(|k\rangle\langle l|) \Big\| = \Big\| \sum_{x,y} (E_A^x)^{\frac{1}{2}} (F_A^y)(E_A^x)^{\frac{1}{2}} \otimes |y\rangle\langle y| \otimes |x\rangle\langle x| \Big\| \\ &\leq \max_{x,y} \Big\| (E_A^x)^{\frac{1}{2}} \cdot (F_A^y)^{\frac{1}{2}} \Big\|^2 \ . \end{aligned}$$

7. Privacy Amplification against Quantum Adversaries

A basic task in cryptography is to create a secure key from a classical random variable, which might be initially correlated to an adversary. Privacy amplification is the answer to this problem in the sense that it gives you an algorithm how to compute a secure key, and furthermore, the amount of key you get is essentially optimal. A crucial question is how one models the system of the adversary. In classical cryptography one usually assumes that the adversary's information is purely classical. The security in this scenario was analyzed in [10, 51, 8, 76]. In quantum cryptography one goes a step further and allows the adversary to encode his information in a state of a finite-dimensional quantum system. Security in this regime was analyzed in [53, 74, 72, 93]. Furthermore, one can use the techniques of [40] to extend these results to the case when the adversary holds a state of a quantum system which is described by a separable Hilbert space $\mathcal{H}$ [39].

Here we consider the case when the adversary's information is encoded in a state of a quantum system which is described by a general von Neumann algebra $\mathcal{M}$. This generalizes the result of privacy amplification to the most general quantum setting. If it comes to practical applications, this result might not be essential for systems with an infinite number of degrees of freedom, even if these are modeled by von Neumann algebras, because the results in [39] and a simple embedding argument are in fact sufficient. But in general this goes hand in hand with a potentially shorter key length and might therefore not be favorable. We will discuss this arguments at the end of this section in greater detail once the notation is settled.

A classical random variable X correlated to some quantum state on a von Neumann algebra $\mathcal{M}_E$ can be modeled by a classical quantum state ω_{XE} on $\ell^\infty(X) \otimes \mathcal{M}_E$. A perfectly secure key now corresponds to a uniform distribution that is independent of the adversary's information. This is described by a classical quantum state

$$\frac{1}{|X|} e_X \otimes \sigma_E \ ,$$

where $e_X = (1, \ldots, 1) \in \ell^1(X)$ and $\sigma_E \in \mathcal{S}(\mathcal{M}_E)$. In general, it is impossible to extract a perfectly secure key and therefore we concentrate on ϵ-secure keys. The following security definition is analogue to the finite-dimensional case [72] and inherits all desired properties (see [72, Section 2.2] for a detailed discussion).

Definition 7.1. *Let $\mathcal{M}_E$ be a von Neumann algebra, X a set of finite cardinality $|X|$, $\omega_{XE} = \oplus_{x\in X}\omega_E^x \in \ell^1(X)\otimes\mathcal{S}_\leq(\mathcal{M}_E)$, and $\varepsilon \geq 0$. Then ω_{XE} is called an ϵ-secure key with respect to $\mathcal{M}_E$ if*

$$\|\omega_{XE} - \frac{1}{|X|}e_X\otimes\omega_E\|_{\ell^1(\mathcal{N}(\mathcal{M}_E))} \leq \epsilon \ ,$$

where $\omega_E = \sum_{x\in X}\omega_E^x$.

Henceforth, we omit the subscript $\ell^1(\mathcal{N}(\mathcal{M}_E))$ for the norm. The basic idea to achieve an ϵ-secure key from an input ω_{XE} is to randomly combine several indices x into a single one, and thereby reducing the alphabet from X to K with $|K| < |X|$. This process can be accomplished by using two-universal hash functions.

Definition 7.2. *Let X, K be sets of finite cardinality such that $|K| \leq |X|$. A family of $\{X,K\}$-hash functions is a set $\{\mathcal{F},\mathbb{P}_\mathcal{F}\}_{X,K}$, where every element $f\in\mathcal{F}$ is a function $f: X\to K$, called hash function, and $\mathbb{P}_\mathcal{F}$ is a probability measure on the set $\mathcal{F}$. A family of $\{X,K\}$-hash functions is called two-universal if for all $x,y\in X$ with $x\neq y$*

$$\mathbb{P}_\mathcal{F}\left(f(x)=f(y)\right) \leq \frac{1}{|K|} \ . \tag{41}$$

Proposition 7.3. [24, 98] *Let X, K be sets of finite cardinality such that $|K| \leq |X|$. Then there exists a family of two-universal $\{X,K\}$-hash functions.*

Given a family of $\{X,K\}$-hash functions, we now construct maps which implement the action of hash functions f on probability distributions. That is, we define the operators T_f from $\ell^1(X)$ to $\ell^1(K)$ by

$$(T_f u)(i) = \sum_{x\in X: f(x)=i} u(x) \ , \quad u\in\ell^1(X),\ i\in K. \tag{42}$$

The action of the operators T_f can then trivially be extended to the space $\ell^1(X)\otimes\mathcal{S}_\leq(\mathcal{M}_E)$ by

$$T_f\otimes\mathrm{id} : \ell^1(X)\otimes\mathcal{S}_\leq(\mathcal{M}_E) \to \ell^1(K)\otimes\mathcal{S}_\leq(\mathcal{M}_E) \tag{43}$$

$$(T_f\otimes\mathrm{id})(\omega_{XE})(i) = \sum_{x\in X: f(x)=i}\omega_E^x \ , \quad i\in K \ , \tag{44}$$

where $\omega_{XE} = \oplus_{x\in X}\omega_E^x$.

Theorem 7.4. *Let $\mathcal{M}_E$ be a von Neumann algebra, X, K sets of finite cardinality with $|K| \leq |X|$, $\{\mathcal{F},\mathbb{P}_\mathcal{F}\}_{X,K}$ a family of two-universal $\{X,K\}$-hash functions, and $\omega_{XE} = \oplus_{x\in X}\omega_E^x \in \ell^1(X)\otimes\mathcal{S}_\leq(\mathcal{M}_E)$. Furthermore denote by $\mathbb{E}_\mathcal{F}$ the expectation with respect to $\mathbb{P}_\mathcal{F}$ and by $(T_f\otimes\mathrm{id})$ the operator given in* (44)*. Then*

$$\mathbb{E}_\mathcal{F}\|(T_f\otimes\mathrm{id})(\omega_{XE}) - \frac{1}{|K|}e_K\otimes\omega_E\| \leq \sqrt{|K|\cdot 2^{-\mathrm{H}_{\min}(X|E)_\omega}} \ ,$$

where $\omega_E = \sum_x \omega_E^x \in \mathcal{S}_\leq(\mathcal{M}_E)$.

Proof. The proof is different from the finite dimensional ones in [72, 93] and is more along the line of the classical results [10, 51, 8]. The norm on $\ell^1(\mathcal{N}(\mathcal{M}_E))$ is defined to be the dual norm of $\ell^\infty(X)\otimes\mathcal{M}_E$, and hence we have to consider the expectation value $\mathbb{E}_\mathcal{F}$ of the following expression

$$\|(T_f\otimes\mathrm{id})(\omega_{XE}) - \frac{1}{|K|}e_K\otimes\omega_E\| = \sum_{i\in K}\sup_{a_i\in\mathcal{M}_E,\|a_i\|=1}\left|\sum_{x\in X: f(x)=i}\omega_E^x(a_i) - \frac{1}{|K|}\omega_E(a_i)\right| \ . \tag{45}$$

Because $\mathrm{H}_{\min}\left(X|E\right)_\omega$ is finite (see Section 4.3), we can assume that there exists a $\sigma_E\in\mathcal{S}(\mathcal{M}_E)$ such that $\omega_E^x \leq \lambda\cdot\sigma_E$ for all $x\in X$ and suitable $\lambda > 0$. We choose $(\pi_\sigma,\mathcal{H}_\sigma,\xi_\sigma)$ to be a purification of σ_E,

and denote by $D_x \in \pi_\sigma(\mathcal{M}_E)'$ (resp. $D \in \pi_\sigma(\mathcal{M}_E)'$) the corresponding Radon-Nikodym derivatives of ω_E^x (resp. ω_E) with respect to σ (see Appendix B). Using D_x, D we can write

$$\sum_{x\in X:f(x)=i} \omega_E^x(a_i) - \frac{1}{|K|}\omega_E(a_i) = \sum_{x\in X:f(x)=i} \langle \xi_\sigma \,|D_x^* D_x\, \pi_\sigma(a_i)\xi_\sigma \,\rangle - \frac{1}{|K|}\,\langle \xi_\sigma \,|D^* D\, \pi_\sigma(a_i)\xi_\sigma \,\rangle$$
$$= \,\langle \left(\sum_{x\in X:f(x)=i} D_x^* D_x - \frac{1}{|K|} D^* D \right) \xi_\sigma \,|\pi_\sigma(a_i)\xi_\sigma \,\rangle \;,$$

where the last step follows from the fact that D_x as well as D are elements of the commutant of $\pi_\sigma(\mathcal{M}_E)$. We now insert this expression into (45), take the expectation $\mathbb{E}_\mathcal{F}$ and apply the following estimate, which follows from a two-fold application of the Cauchy-Schwarz inequality,

$$\mathbb{E}_\mathcal{F} \sum_{i\in K} |\,\langle \varphi_{i,f} \,|\psi_{i,f}\,\rangle| \leq \left(\mathbb{E}_\mathcal{F} \sum_{i\in K} \langle \varphi_{i,f} \,|\varphi_{i,f}\,\rangle \right)^{\frac{1}{2}} \left(\mathbb{E}_\mathcal{F} \sum_{i\in K} \langle \psi_{i,f} \,|\psi_{i,f}\,\rangle \right)^{\frac{1}{2}} .$$

We find that the expression of interest, namely $\mathbb{E}_\mathcal{F} \|(T_f \otimes \mathrm{id})(\omega_{XE}) - \frac{1}{|K|} e_K \otimes \omega_E\|$, can be bounded by the quantity

$$\sqrt{|K|} \left(\mathbb{E}_\mathcal{F} \sum_{i\in K} \langle \xi_\sigma \,| \left(\sum_{x\in X:f(x)=i} D_x^* D_x - \frac{1}{|K|} D^* D \right)^2 \xi_\sigma \,\rangle \right)^{\frac{1}{2}} ,$$

where the term $\sqrt{K}$ originates from the estimate $\sum_{i\in K} \sup_{a_i \in \mathcal{M}_E, \|a_i\|=1} \langle \xi_\sigma \,|\pi_\sigma(a_i)^* \pi_\sigma(a_i)\xi_\sigma \,\rangle \leq K$. So we are left with the expression under the square root. A simple binomial identity leads to

$$\mathbb{E}_\mathcal{F} \sum_{i\in K} \langle \xi_\sigma \,| \left(\sum_{x\in X:f(x)=i} D_x^* D_x - \frac{1}{|K|} D^* D \right)^2 \xi_\sigma \,\rangle \tag{46}$$

$$= \mathbb{E}_\mathcal{F} \sum_{i\in K} \langle \xi_\sigma \,| \left(\sum_{x\in X:f(x)=i} D_x^* D_x \right)^2 \xi_\sigma \,\rangle - \frac{1}{|K|}\,\langle \xi_\tau \,|D^* D D^* D \xi_\sigma \,\rangle \;. \tag{47}$$

Here we used two identities, the first one being

$$\mathbb{E}_\mathcal{F} \sum_{i\in K} \sum_{x\in X:f(x)=i} \equiv \sum_{x\in X} ,$$

and the second one following from a lemma about the Radon-Nikodym derivative of classical quantum states (Lemma B.3)

$$\sum_{x\in X} D_x^* D_x \xi_\sigma = D^* D \xi_\sigma \;. \tag{48}$$

We proceed by considering the first term in the binomial expansion applied above, and find that

$$\left(\sum_{x\in X:f(x)=i} D_x^* D_x \right)^2 = \sum_{x\in X:f(x)=i} \sum_{y\in X:f(y)=i} D_x^* D_x D_y^* D_y$$
$$= \sum_{x\in X} \sum_{y\in X} (1-\delta_{x,y})\, \delta_{f(x)=i}\, \delta_{f(y)=i}\, D_x^* D_x D_y^* D_y \;+ \sum_{x\in X:f(x)=i} D_x^* D_x D_x^* D_x \;.$$

Next we have to take the expectation value of the last expression. The only quantities depending on the hashing function f are now the three deltas $(1-\delta_{x,y})\,\delta_{f(x)=i}\,\delta_{f(y)=i}$. Using the fact that $\mathcal{F}$ is a family of two-universal hash functions (Definition 7.2), we find that their expectation value fulfills

$$\mathbb{E}_\mathcal{F} \left(\sum_{i\in K} (1-\delta_{x,y})\, \delta_{f(x)=i}\, \delta_{f(y)=i} \right) \leq \frac{1}{|K|} \;.$$

Hence we get the following bound for the quadratic term in (46),

$$\mathbb{E}_{\mathcal{F}} \sum_{i\in K} \langle \xi_\sigma \,|\, \left(\sum_{x\in X: f(x)=i} D_x^* D_x \right)^2 \xi_\sigma \,\rangle \leq \sum_{x\in X} \langle \xi_\sigma \,|D_x^* D_x D_x^* D_x \xi_\sigma \,\rangle + \frac{1}{|K|} \langle \xi_\sigma \,|D^* D D^* D \xi_\sigma \,\rangle \ ,$$

where we again used (48). Inserting this into (46), we see that the second term is cancelled, and thus we are left with the bound

$$\mathbb{E}_{\mathcal{F}} \sum_{i\in K} \langle \xi_\sigma \,|\, \left(\sum_{x\in X: f(x)=i} D_x^* D_x - \frac{1}{|K|} D^* D \right)^2 \xi_\sigma \,\rangle \leq \sum_{x\in X} \langle \xi_\sigma \,|D_x^* D_x D_x^* D_x \xi_\sigma \,\rangle \ .$$

The expression on the right hand side can be estimated further, since we know that due to the Lemma B.3 and the definition of Radon-Nikodym derivatives $\langle \xi_\sigma \,|\, \sum_{x\in X} D_x^* D_x \xi_\sigma \,\rangle = \omega_E(\mathbb{1}) \leq 1$. Hence we find

$$\sum_{x\in X} \langle \xi_\sigma \,|D_x^* D_x D_x^* D_x \xi_\sigma \,\rangle \leq \max_{x\in X} \|D_x^* D_x\| \, \langle \xi_\sigma \,|\, \sum_{x\in X} D_x^* D_x \xi_\sigma \,\rangle \leq 2^{\mathrm{D}_{\max}\left(\oplus_x \omega_E^x || \oplus_x \sigma_E\right)} \ ,$$

where the last step follows from Proposition B.2 and the definition of the max-relative entropy. This leaves us with the estimate

$$\mathbb{E}_{\mathcal{F}} \|(T_f \otimes \mathrm{id})(\omega_{XE}) - \frac{1}{|K|} e_K \otimes \omega_E\| \leq \sqrt{|K| \cdot 2^{\mathrm{D}_{\max}\left(\oplus_x \omega_E^x || \oplus_x \sigma_E\right)}} \ .$$

Finally, since our considerations are valid for all suitable $\sigma_E \in \mathcal{S}(\mathcal{M}_E)$, the assertion follows easily by taking the infimum over this set and inserting the definition of the min-entropy of classical quantum states. □

This theorem can be strengthened further to the following.

Corollary 7.5. *For the same conditions as in Theorem 7.4 and $\epsilon \geq 0$, it holds that*

$$\mathbb{E}_{\mathcal{F}} \|(T_f \otimes \mathrm{id})(\omega_{XE}) - \frac{1}{|K|} e_K \otimes \omega_E\| \leq \sqrt{|K| \cdot 2^{-\mathrm{H}_{\min}^\epsilon(X|E)_\omega}} + 4\epsilon \ ,$$

where $\omega_E = \sum_x \omega_E^x \in \mathcal{S}(\mathcal{M}_E)$.

Proof. The idea of the proof is exactly the same as in [72, 93], but we repeat the argument for completeness. By the definition of the smooth conditional min-entropy (Defintion 4.11), for any $\delta > 0$, there exists $\bar{\omega}_{XE} \in \mathcal{B}^\epsilon(\omega_{XE})$ such that

$$\mathrm{H}_{\min}(X|E)_{\bar{\omega}} \geq \mathrm{H}_{\min}^\epsilon(X|E)_\omega - \delta \ .$$

By Lemma 4.8, $\bar{\omega}_{XE} \in \mathcal{B}^\epsilon(\omega_{XE})$ implies $\|\bar{\omega}_{XE} - \omega_{XE}\| \leq 2\epsilon$, and moreover it is easy to see that by the definition of the norm (see equation (2)) and the definition of the operator $T_f \otimes \mathrm{id}$ (see (44)), it follows that

$$\|(T_f \otimes \mathrm{id})(\bar{\omega}_{XE}) - (T_f \otimes \mathrm{id})(\omega_{XE})\| \leq 2\epsilon \ .$$

Using the triangle inequality and Theorem 7.4, we can conclude that

$$\begin{aligned} \mathbb{E}_{\mathcal{F}} \|(T_f \otimes \mathrm{id})(\omega_{XE}) - \frac{1}{|K|} e_K \otimes \omega_E\| &\leq \mathbb{E}_{\mathcal{F}} \|(T_f \otimes \mathrm{id})(\bar{\omega}_{XE}) - \frac{1}{|K|} e_K \otimes \bar{\omega}_E\| \\ &\quad + \|(T_f \otimes \mathrm{id})(\bar{\omega}_{XE}) - (T_f \otimes \mathrm{id})(\omega_{XE})\| + \|\bar{\omega}_E - \omega_E\| \\ &\leq \sqrt{|K| \cdot 2^{-\mathrm{H}_{\min}(X|E)_{\bar{\omega}}}} + 4\epsilon \leq \sqrt{|K| \cdot 2^{-\mathrm{H}_{\min}^\epsilon(X|E)_\omega + \delta}} + 4\epsilon \ . \end{aligned}$$

Because this holds for any $\delta > 0$, the claim follows. □

Now privacy amplification for given $\omega_{XE} \in \ell^1(X) \otimes \mathcal{S}(\mathcal{M}_E)$ and $\epsilon > 0$ works as follows. We choose

$$|K| = \lfloor 2^{\mathrm{H}_{\min}^{\epsilon/5}(X|E)_\omega - 2\log\frac{5}{\epsilon}} \rfloor \ . \tag{49}$$

and apply a hash function chosen from a two-universal family of $\{X, K\}$-hash functions according to the distribution $\mathbb{P}_{\mathcal{F}}$. A straightforward calculation shows that by Corollary 7.5, we get an ϵ-secure

key with respect to $\mathcal{M}_E$ of length given in (49). As a next step we show that this amount is also essentially optimal.

Proposition 7.6. *Let $\mathcal{M}_E$ be a von Neumann algebra, X, K sets of finite cardinality with $|K| \leq |X|$, and $f : X \mapsto K$. If $\omega_{XE} = \oplus_{x\in X}\omega_E^x \in \ell^1(X) \otimes \mathcal{S}(\mathcal{M}_E)$ is such that $\omega_{f(X)E} = \frac{1}{|K|}e_K \otimes \sigma_E$ for some $\sigma_E \in \mathcal{S}(\mathcal{M}_E)$, then*

$$\log |K| \leq \mathrm{H}_{\min}(X|E)_\omega \ .$$

Proof. The idea of the proof is exactly the same as in [93], but we repeat the argument for completeness. By the definition of the guessing probability (32), it is easily seen that the probability for the adversary to guess K can not be smaller than the probability to guess X, that is,

$$p_{\text{guess}}(X|E)_\omega \leq p_{\text{guess}}(K|E)_\omega \ .$$

Furthermore, $p_{\text{guess}}(K|E) = 2^{-\log|K|}$ and by the operational interpretation of the min-entropy of classical quantum states as the guessing probability (Proposition 5.4) we conclude that

$$\mathrm{H}_{\min}(X|E)_\omega = -\log p_{\text{guess}}(X|E)_\omega \geq -\log p_{\text{guess}}(K|E)_\omega = \log|K| \ .$$

□

Hence, for any given classical quantum state ω_{XE}, it is impossible to extract more than $\mathrm{H}_{\min}(X|E)_\omega$ bits of perfect key. We generalize this to the case of an ϵ-perfect key.[21]

Corollary 7.7. *Let $\mathcal{M}_E$ be a von Neumann algebra, X, K sets of finite cardinality with $|K| \leq |X|$, $f : X \mapsto K$, and $\varepsilon \geq 0$. If $\omega_{XE} = \oplus_{x\in X}\omega_E^x \in \ell^1(X)\otimes\mathcal{S}(\mathcal{M}_E)$ is such that $\|\omega_{f(X)E} - \frac{1}{|K|}e_K\otimes\sigma_E\| \leq \epsilon$ for some $\sigma_E \in \mathcal{S}(\mathcal{M}_E)$, then*

$$\log|K| \leq \mathrm{H}_{\min}^{\sqrt{\epsilon}}(X|E)_\omega \ .$$

Proof. By Lemma 4.8, $\|\omega_{f(X)E} - \frac{1}{|K|}e_K \otimes \sigma_E\| \leq \epsilon$ implies

$$\omega_{f(X)E} \approx_{\sqrt{\epsilon}} \frac{1}{|K|}e_K \otimes \sigma_E \ .$$

Furthermore, by the definition of the smooth conditional min-entropy (Defintion 4.11), for any $\delta > 0$ exists a cq-state $\bar{\omega}_{KE} \in \mathcal{B}^{\sqrt{\epsilon}}(\omega_{f(X)E})$ such that

$$\mathrm{H}_{\min}(K|E)_{\bar{\omega}} \geq \mathrm{H}_{\min}^{\sqrt{\epsilon}}(K|E)_\omega - \delta \ .$$

We define $\tilde{T}_f : \mathcal{N}(M_{|X|}) \to \ell^1(K)$ as the concatenation of the measurement in the diagonal basis $|x\rangle\langle x|$, $x \in X$, and applying the function f on x. If we show that there exists a preimage $\bar{\omega}_{XE}$ of $\bar{\omega}_{KE}$ under $\tilde{T}_f \otimes \mathrm{id}$ which satisfies $\bar{\omega}_{XE} \approx_{\sqrt{\epsilon}} \omega_{XE}$, we obtain

$$\mathrm{H}_{\min}^{\sqrt{\epsilon}}(X|E)_\omega \geq \mathrm{H}_{\min}(X|E)_{\bar{\omega}} \geq \mathrm{H}_{\min}(K|E)_{\bar{\omega}} \geq \mathrm{H}_{\min}^{\sqrt{\epsilon}}(K|E)_\omega - \delta \geq \log|K| - \delta \ , \tag{50}$$

where the second inequality is due to Proposition 7.6. Because this holds for any $\delta > 0$, the claim follows. Hence, it remains to prove the existence of such a state $\bar{\omega}_{XE}$. $\tilde{T}_f$ is a quantum channel, thus completely positive and unital, and it has a Stinespring dilation [62], $V_X : \mathbb{C}^{|X|} \to \mathbb{C}^{|K|}\otimes\mathbb{C}^{|X|}$, which is given by $V_X = \sum_x |f(x)\rangle_K \otimes |x\rangle\langle x|_{X''}$. Here, the ancilla of the dilation is denoted by X''. Applied on a state $\sigma_{EX} \in \mathcal{S}(M_{|X|} \otimes \mathcal{M}_E)$, this means that $(\tilde{T}_f \otimes \mathrm{id})(\sigma_{XE})$ is the restriction of the state $V_X^*\sigma_{XB}V_X(a) = \sigma_{XB}\big((V_X^* \otimes \mathbb{1}_E)x(V_X \otimes \mathbb{1})\big)$ onto system K and E, where $a \in \mathcal{M}_X \otimes \mathcal{M}_E$. Now let $\omega_{XX'EE'}$ be a purification $(\pi, \mathcal{H}, |\xi_\omega\rangle)$ of the cq-state ω_{XE}, where $\mathcal{H} = \mathbb{C}^{|X|}\otimes\mathbb{C}^{|X|}\otimes\mathcal{H}_{EE'}$. Then it follows that $|\xi_\omega^V\rangle = V_X \otimes \mathbb{1}_X \otimes \mathbb{1}_{EE'}|\xi_\omega\rangle$ is a purification of ω_{KE} in $\mathcal{H}' = \mathbb{C}^{|K|}\otimes\mathcal{H}$, since the restriction of $\omega_{KX''X'EE'} = V_X^*\omega_{XX'EE'}V_X$ onto system K and E is ω_{KE}. Now we take $\bar{\omega}_{KE} \approx_{\sqrt{\epsilon}} \omega_{KE}$ as defined above and note that this implies $F(\omega_{KE}, \bar{\omega}_{KE}) \geq 1 - \epsilon$. We can chose the representation π and the

[21] We were not able to find a detailed proof about this for the finite-dimensional case, although the optimality is mentioned in [72, 93].

Hilbert space $\mathcal{H}_{EE'}$ in such way that $\bar{\omega}_{KE}$ has a purification $|\xi_{\bar{\omega}}\rangle$ in $\mathcal{H}'$, because we can always go into the standard form (see Appendix A). Then we obtain by the definition of the fidelity

$$F(\omega_{KE}, \bar{\omega}_{KE}) = \sup_{U \in \pi(\mathcal{M}_{KE})', \|U\| \leq 1} F_{\mathcal{B}(\mathcal{H}')}(|\xi^V_\omega\rangle, U|\xi_{\bar{\omega}}\rangle) \ . \tag{51}$$

Let $p = V_X^* V_X$ be the projector onto the image of V_X and observe that for all $U \in \pi(\mathcal{M}_{KE})'$

$$F(p|\xi^V_\omega\rangle, U|\xi_{\bar{\omega}}\rangle) = F(|\xi^V_\omega\rangle, pU|\xi_{\bar{\omega}}\rangle) \ . \tag{52}$$

We can therefore conclude that the optimum is attained for a purification $|\xi^{op}_{\bar{\omega}}\rangle$ in $p\mathcal{H}'$. Because $V : \mathcal{H} \to p\mathcal{H}'$ is unitary, and the fidelity is invariant under unitary transformation, we obtain

$$1 - \epsilon \leq F(\omega_{KE}, \bar{\omega}_{KE}) = F_{\mathcal{B}(p\mathcal{H}')}(|\xi^V_\omega\rangle, |\xi^{op}_{\bar{\omega}}\rangle) = F_{\mathcal{B}(\mathcal{H})}((V_X^* \otimes \mathbb{1})|\xi_\omega\rangle, (V_X^* \otimes \mathbb{1})|\xi^{op}_{\bar{\omega}}\rangle) \leq F(\omega_{XE}, \bar{\omega}_{XE}) \ .$$

where $\bar{\omega}_{XE}$ is the restriction onto $\mathcal{M}_{XE}$ of the state corresponding to $(V_X^* \otimes \mathbb{1})|\xi^{op}_{\bar{\omega}}\rangle$. Note that the last equality is due to the monotonicity of the fidelity (14). By construction $\tilde{T}_f$ maps $\bar{\omega}_{XE}$ to $\bar{\omega}_{KE}$ and therefore we found the desired state. □

Now we come back to the discussion of how one can apply the results for privacy amplification in the case of quantum systems described by finite-dimensional [72, 93] or separable [39] Hilbert spaces to the case where the system is modeled by a von Neumann algebra. The following idea is from [25]. If the eavesdropper's von Neumann algebra $\mathcal{M}_E$ is not a full $\mathcal{B}(\mathcal{H})$, then it can be naturally embedded into a full $\mathcal{B}(\mathcal{H}) \equiv \mathcal{M}_{\bar{E}}$. By the definition of a key (Definition 7.1) and $\mathcal{M}_E \subseteq \mathcal{M}_{\bar{E}}$, an ϵ-secure key with respect to $\mathcal{M}_{\bar{E}}$ is also an ϵ-secure key with respect to $\mathcal{M}_E$.[22] If $\mathcal{H}$ is separable the result from [39] can be applied, which provides a secure key of length $\mathrm{H}^\epsilon_{\min}(X|\bar{E})_\omega$, where $\omega_{X\bar{E}}$ is any extension of ω_{XE} on $\mathcal{M}_{X\bar{E}}$. We note that it might be possible to generalize the techniques of [40] to non-separable Hilbert spaces [96].

For many physical systems one can even overcome this requirement by using the following argument. Namely, if the adversary's von Neumann algebra has a property called hyperfinite, which basically means that the von Neumann algebra can be arbitrarily well approximated by a direct sum of finite-dimensional matrix algebras (see [82] for proper definitions).[23] Although this is a non-constructive property, it is enough for privacy amplification. This is because we do not care about how the eavesdropper actually looks like, but only how it can be described in principle. Of course, we again have the problem that a direct sum of finite-dimensional matrix algebras is in general not a full $\mathcal{B}(\mathcal{H})$, but it can be embedded into a $\mathcal{B}(\mathcal{H})$ for some finite-dimensional Hilbert space $\mathcal{H}$, for which the privacy amplification result for finite-dimensional Hilbert spaces is sufficient.

But all these arguments rely on an embedding argument, and hence one generally loses the tightness of the privacy amplification result, and therefore, the optimality of the key length. This is also suggested by the data processing inequality (Proposition 4.15), which reads

$$\mathrm{H}^\epsilon_{\min}(X|E)_\omega \geq \mathrm{H}^\epsilon_{\min}(X|\bar{E})_\omega \ .$$

Of course, a natural question is to ask for the amount of the loss. This is also interesting in a more general perspective since it is directly linked to restrictions of possible measurements of the eavesdropper. We end with the remark that the embedding argument might not work for general cryptographic setups with many parties. This is because of Tsirelson's problem [94, 59, 52, 82, 58], or more precisely its generalization to many parties, which makes it unclear how one should embed all parties individually.

[22] This follows from the monotonicity of the norm on $\mathcal{N}(\mathcal{M})$ under quantum channels.

[23] Hyperfinite von Neumann algebras include in particular the free boson field of finite temperature [4], and hyperfiniteness is also a consequence of certain axioms in algebraic quantum field theory [18].

8. Classical Data Compression with Quantum Side Information

The question of how much a classical random variable can be compressed is one of the most fundamental task in classical information theory, and the answer goes all the way back to the pioneering work of Shannon [84]. Here we are interested in a particular version of the problem, where a classical random variable X is with a classical party Alice, but correlated with another party Bob, who is of general quantum nature. The question is then how many bits that Alice needs to send to Bob, such that he can recover X, using his quantum side information and the classical message. Under the assumption that the classical variable has finite alphabet, and that Bob's system can be modeled using a finite dimensional Hilbert space, this scenario was first analyzed in the asymptotic iid regime in [34],[24] but recently also generalized to the one-shot case [70]. This then corresponds to the question as stated above.

In our work we consider the scenario when Bob's side information is encoded in a state of a quantum system, which is described by a general von Neumann algebra $\mathcal{M}_B$, whereas the classical random variable still has finite alphabet size.[25] Note that this is not a cryptographic task so far, but nevertheless the task is interesting for quantum cryptography, because together with the result about privacy amplification against quantum adversaries (Section 7), it allows the abstract quantification of distillable key (Section 9).

A classical random variable X correlated to some quantum state on a von Neumann algebra $\mathcal{M}_B$ is modeled by a cq-state $\omega_{XB} \in \mathcal{S}(\ell^\infty_{|X|} \otimes \mathcal{M}_B)$. A one-way classical communication protocol to transmit the random variable X from Alice to Bob then consists of a classical encoding map $\mathcal{E} : \ell^1(X) \to \ell^1(C)$ on Alice's side, and a decoding map $\mathcal{D} : \ell^1(C) \otimes \mathcal{N}(\mathcal{M}_B) \to \ell^1(X)$ on Bob's side, where the classical alphabet C specifies the number of bits, $\log|C|$, that are transmitted. The decoding map can be written as $\mathcal{D} = \{\mathcal{D}^c\}_{c\in C}$, where the quantum channel $\mathcal{D}^c$ onto the classical outcome X can be described by a POVM $\{D^c_x\}_{x\in X}$. In particular, this means that if Bob receives the value $c \in C$ from Alice he performs the measurement $\{D^c_x\}$, and declares the measurement outcome to be his guess of the value hold by Alice. In the following every such protocol is specified by the triple $(\mathcal{E}, \mathcal{D}, C)$.

Definition 8.1. *Let $\mathcal{M}_B$ be a von Neumann algebra, X a set of finite cardinality $|X|$, and $\omega_{XB} \in \mathcal{S}(\ell^\infty_{|X|} \otimes \mathcal{M}_B)$. Then, the error probability of a protocol $(\mathcal{E}, \mathcal{D}, C)$ for ω_{XB} is given by*

$$p_{\mathrm{err}}(\omega_{XB}; \mathcal{E}, \mathcal{D}) = 1 - \sum_x \omega^x_B(D^{\mathcal{E}(x)}_x) \ , \tag{53}$$

and a protocol is called ϵ-reliable if $p_{\mathrm{err}}(\omega_{XB}; \mathcal{E}, \mathcal{D}) \leq \epsilon$.

The main technical result of this section is the following quantification of the achievable error probability, as it was already shown for the finite-dimensional case in [70].

Theorem 8.2. *Let $\mathcal{M}_B$ be a von Neumann algebra, X a set of finite cardinality $|X|$, and $\omega_{XB} \in \mathcal{S}(\ell^\infty_{|X|} \otimes \mathcal{M}_B)$. Then there exist for any alphabet C with $|C| \leq |X|$, an encoding map $\mathcal{E}$ and a decoding map $\mathcal{D}$, such that the protocol $(\mathcal{E}, \mathcal{D}, C)$ satisfies*

$$p_{\mathrm{err}}(\omega_{XB}; \mathcal{E}, \mathcal{D}) \leq \sqrt{\frac{1}{|C|} \cdot 2^{\mathrm{H}_{\max}(X|B)_\omega + 3}} \ . \tag{54}$$

The protocol for which the bound is achieved, is in complete analogy to the finite-dimensional version [70]. We start by sketching the idea. For the encoding we employ the property of a family of two-universal hash functions $\mathcal{F}$ (Definition 7.2). In particular, we show that the averaged error probability over a family of two-universal hash functions $\mathcal{F}$ is bounded as in Equation (54). From

[24] Here asymptotic iid means that one has many independent copies of X and asks for the average asymptotic rate of classical communication needed.

[25] From the perspective of quantum cryptography this is a reasonable assumption.

this we can then conclude that there exists a function $f \in \mathcal{F}$ suitable as an encoding map. Now assume that Alice holds the value x and sends the message $c = f(x)$ to Bob. Bob then knows that $x \in f^{-1}(c)$, and applies as the decoding map a measurement which is appropriate to distinguish between the states ω_B^x for $x \in f^{-1}(c)$. For that, he uses a POVM $\{D^c_{x';f}\}_{x' \in X}$ with $D^c_{x';f} = 0$ if $x' \notin f^{-1}(c)$, which we choose as an adapted 'pretty good measurement' [43] to distinguish the ensemble $\{\omega_B^x\}_{x \in f^{-1}(c)}$.

Proof. The proof is based on Lemmata C.1 and C.2, and is similar to the one for the finite-dimensional case [70] (except for some technical difficulties). Let $\{\mathcal{F}, \mathbb{P}_{\mathcal{F}}\}_{X,C}$ be a family of two-universal hash functions from the alphabet X onto C (Definition 7.2). We define Π_x to be the support projection onto the positive part of $\omega_B^x - 2^{-m-1}\omega_B$, where $\omega_B = \sum_x \omega_B^x$. Note that $\Pi_x \in \mathcal{M}_B$ for all $x \in X$.

Since the Hilbert space $\mathcal{H}_B$ on which $\mathcal{M}_B$ acts is in general infinite-dimensional, we have to introduce some regularizing terms, parameterized in ϵ, in order to apply Lemma C.1.[26] For any $f \in \mathcal{F}$ and $c \in C$, we define for $\epsilon > 0$ and $x \in f^{-1}(c)$

$$S^c_{x;f}(\epsilon) := \frac{\Pi_x + \epsilon \mathbb{1}}{1 + \epsilon |f^{-1}(c)|} \text{ and } T^c_{x;f}(\epsilon) := \Big(\sum_{x' \in X} \Pi_{x'} \delta_{x'c} + \epsilon |f^{-1}(c)| \mathbb{1} \Big) - S^c_{x;f}(\epsilon) \ .$$

It is straightforward to see that $S^c_{x;f}(\epsilon) + T^c_{x;f}(\epsilon)$ is invertible for any $\epsilon > 0$ and $x \in f^{-1}(c)$. By the help of these operators, we now define an ϵ-family of decoding measurements $\{D^c_{x;f}(\epsilon)\}_{x \in X}$ conditioned on the fact that the encoding map is $f \in \mathcal{F}$ and the obtained message is c via

$$D^c_{x;f}(\epsilon) = \big(S^c_{x;f}(\epsilon) + T^c_{x;f}(\epsilon)\big)^{-\frac{1}{2}} S^c_{x;f}(\epsilon) \big(S^c_{x;f}(\epsilon) + T^c_{x;f}(\epsilon)\big)^{-\frac{1}{2}} \ ,$$

if $x \in f^{-1}(c)$ and $D^c_{x;f}(\epsilon) = 0$ else. For any $\epsilon > 0$ it is true that $D^c_{x;f}(\epsilon)$ is a positive operator in $\mathcal{M}_B$ and $\sum_x D^c_{x;f}(\epsilon) \leq \mathbb{1}$. Hence, $\{D^c_{x;f}(\epsilon)\}_{x \in X}$ defines a valid but possibly incomplete measurement. On the other side, one can check that by setting $S = S^c_{x;f}(\epsilon)$ and $T = T^c_{x;f}(\epsilon)$ the conditions in Lemma C.1 are satisfied, from which we obtain that

$$\mathbb{1} - D^c_{x;f}(\epsilon) \leq 2(\mathbb{1} - S^c_{x;f}(\epsilon)) + 4T^c_{x;f}(\epsilon) \ . \tag{55}$$

Now, the idea is to define the particular measurements $D^c_{x';f}$ of the decoding map as the 'limit' of $D^c_{x;f}(\epsilon)$ for $\epsilon \to 0$. For that, we consider the sequence $\{D^c_{x;f}(1/n)\}_{n=1}^{\infty}$ in $\mathcal{M}_B$ and observe that it is bounded due to the fact that the elements are measurement operators. In particular, the sequence lies in the unit sphere of $\mathcal{B}(\mathcal{H}_B)$. We can therefore apply the Banach-Alaoglu theorem [67, Theorem VI.26], which says that there exists a σ-weakly converging subsequence $\Lambda \subset \mathbb{N}$ of $\{D^c_{x;f}(1/n)\}_{n=1}^{\infty}$. The limit of this subsequence is now used to define the appropriate measurements at the decoder

$$D^c_{x;f} = \sigma - \lim_{\Lambda \ni n \to \infty} D^c_{x;f}(1/n) \ .$$

Since $\mathcal{M}_B$ is σ-weakly closed, we know that $D^c_{x;f} \in \mathcal{M}_B$, and hence defines a possible measurement in $\mathcal{M}_B$. Because positivity is preserved under taking the σ-weak limit, we obtain from Equation (55) that

$$\mathbb{1} - D^c_{x;f} \leq 2(\mathbb{1} - \Pi_x) + 4 \sum_{x' \notin x} \Pi_{x'} \delta_{x'c} \ , \tag{56}$$

for all $x \in X$. The right hand side of the inequality is obtained by taking the σ-weak limit of $S^c_{x;f}(\epsilon)$ and $T^c_{x;f}(\epsilon)$. If we denote the decoding map corresponding to the measurements $\{D^c_{x;f}\}_{x \in X}$ by $\mathcal{D}^c_f$,

[26] This is in contrast to the finite-dimensional case, where Lemma C.1 is applied directly.

we can bound

$$\begin{aligned}\mathbb{E}_{\mathcal{F}}\Big[p_{\mathrm{err}}(\omega_{XB},f,\mathcal{D}_f^c)\Big] &= \mathbb{E}_{\mathcal{F}}\Big[\sum_x \omega_B^x(\mathbb{1}-D_{x;f}^{f(x)})\Big]\\ &\leq \sum_x \omega_B^x\Big(2(\mathbb{1}-\Pi_x)+\frac{4}{|C|}\sum_{x'}\Pi_{x'}\Big)\\ &= 2\Big[\sum_x \omega_B^x(\mathbb{1}-\Pi_x)+\frac{2}{|C|}\sum_x \omega_B(\Pi_x)\Big]\\ &= 2\Big[\omega_{XB}\Big((\mathbb{1}-\Pi_x)_{x\in X}\Big)+\frac{2}{|C|}\tau_X\otimes\omega_B\Big((\Pi_x)_{x\in X}\Big)\Big]\ .\end{aligned}$$

The first inequality is obtained via the inequality (56) and the defining property (41) of a family of two-universal hash functions. Finally, we apply Lemma C.2 with $\phi=\omega_{XB}$ and $\eta=2/|C|\tau_X\otimes\omega_B$ to obtain

$$\mathbb{E}_{\mathcal{F}}\Big[p_{\mathrm{err}}(\omega_{XB},f,\mathcal{D}_f^c)\Big]\leq 2F\big(\omega_{XB},\frac{2}{|C|}\tau_X\otimes\omega_B\big)^{1/2}\leq\sqrt{\frac{1}{|C|}\cdot 2^{\mathrm{H}_{\max}(X|B)_\omega+3}}\ ,$$

where the last inequality is due to the operational interpretation of the max-entropy as shown in Theorem 5.5. This shows the existence of a suitable $f\in\mathcal{F}$ for which the bound is achieved, and thus completes the proof. □

This theorem can be strengthened further to the following.

Corollary 8.3. *Let $\mathcal{M}_B$ be a von Neumann algebra, X a set of finite cardinality $|X|$, $\omega_{XB}\in\mathcal{S}(\ell^\infty_{|X|}\otimes\mathcal{M}_B)$, and $\epsilon\geq 0$. Then there exist for any alphabet C with $|C|\leq|X|$, an encoding map $\mathcal{E}$ and a decoding map $\mathcal{D}$, such that the protocol $(\mathcal{E},\mathcal{D},C)$ satisfies*

$$p_{\mathrm{err}}(\omega_{XB};\mathcal{E},\mathcal{D})\leq\sqrt{\frac{1}{|C|}\cdot 2^{\mathrm{H}^\epsilon_{\max}(X|B)_\omega+3}}+2\epsilon\ . \tag{57}$$

Proof. The idea of the proof is exactly the same as in [70], but we repeat the argument for completeness. In the following we fix the alphabet C. Let $\mathbb{P}^\omega_{(\mathcal{E},\mathcal{D})}(x,x')$ be the joint probability distribution of the value x hold by Alice and the guess of Bob x', if they use the protocol $(\mathcal{E},\mathcal{D})$, and the source is given by ω_{XB}. A straightforward computation shows that

$$p_{\mathrm{err}}(\omega_{XB},\mathcal{E},\mathcal{D})=\frac{1}{2}\|(\omega_B^x(\mathbb{1})\delta_{xx'})_{x,x'}-(\mathbb{P}^\omega_{(\mathcal{E},\mathcal{D})}(x,x'))_{x,x'}\|_{\ell^1(X\times X)}\ .$$

For any $\delta>0$, we can find a cq-state $\bar\omega_{XB}\in\mathcal{B}^\epsilon(\omega_{XB})$ such that $\mathrm{H}^\epsilon_{\max}(X|B)_\omega\geq\mathrm{H}_{\max}(X|B)_{\bar\omega}-\delta$. If $(\bar{\mathcal{E}},\bar{\mathcal{D}})$ is a protocol for which Theorem 8.2 applies for the state $\bar\omega_{XB}$, we can use the triangle inequality to estimate

$$\begin{aligned}p_{\mathrm{err}}(\omega_{XB},\bar{\mathcal{E}},\bar{\mathcal{D}}) &\leq p_{err}(\omega_{XB},\bar{\mathcal{E}},\bar{\mathcal{D}})+\frac{1}{2}\|(\omega_B^x(\mathbb{1}))_x-(\bar\omega_B^x(\mathbb{1}))_x\|_{\ell^1(X)}\\ &\quad+\frac{1}{2}\|\mathbb{P}^{\bar\omega}_{(\bar{\mathcal{E}},\bar{\mathcal{D}})}(x,x'))_{x,x'}-\mathbb{P}^{\bar\omega}_{(\bar{\mathcal{E}},\bar{\mathcal{D}})}(x,x'))_{x,x'}\|_{\ell^1(X\times X)}\\ &\leq\sqrt{\frac{1}{|C|}\cdot 2^{\mathrm{H}^\epsilon_{\max}(X|B)_\omega+\delta+3}}+\|\bar\omega_{XB}-\omega_{XB}\|\ ,\end{aligned}$$

where we used in the last inequality that the trace distance can only decrease if one applies a quantum channel. Using Lemma 4.8 we can finally bound $\|\bar\omega_{XB}-\omega_{XB}\|\leq 2\epsilon$, from which the result then follows. □

By Corollary 8.3 classical data compression with quantum side information for given $\omega_{XB}\in\mathcal{S}(\ell^\infty(X)\otimes\mathcal{M}_B)$ and error probability $p_{\mathrm{err}}=\epsilon>0$, can now be achieved by sending

$$|C|=\Big\lceil 2^{\mathrm{H}^{\epsilon/2}_{\max}(X|B)_\omega+2\log\frac{1}{\epsilon}+6}\Big\rceil \tag{58}$$

bits from Alice to Bob. As a next step we show that this amount is also essentially optimal.

Lemma 8.4. *Let $\mathcal{M}_B$ be a von Neumann algebra, X a set of finite cardinality $|X|$, $\omega_{XB} \in \mathcal{S}(\ell^\infty_{|X|} \otimes \mathcal{M}_B)$, and $(\mathcal{E}, \mathcal{D}, C)$ be protocol with $p_{\mathrm{err}}(\omega_{XB}, \bar{\mathcal{E}}, \bar{\mathcal{D}}) \leq \epsilon$ for some $\epsilon > 0$. Then*

$$\log |C| \geq \mathrm{H}_{\max}^{\sqrt{2\epsilon}} (X|B)_\omega \ . \tag{59}$$

Proof. The idea of the proof is exactly the same as in [70], but we repeat the argument for completeness. Because of $p_{\mathrm{err}}(\omega_{XB}, \bar{\mathcal{E}}, \bar{\mathcal{D}}) \leq \epsilon$, we know that $\mathbb{P}^\omega_{(\mathcal{E},\mathcal{D})}(x, x')$, as defined in the proof of Corollary 8.3, satisfies $\|\mathbb{P}^\omega_{(\mathcal{E},\mathcal{D})} - \mathbb{P}_{\mathrm{id}}\|_{\ell^1(X\times X)} \leq \epsilon$, where $\mathbb{P}_{\mathrm{id}}(x, x') = \omega_B^x(\mathbb{1})\delta_{xx'}$. Bounding the purified distance by the ℓ^1-norm (Lemma 4.8) and using that $\mathrm{H}_{\max}(X|X')_{\mathbb{P}_{\mathrm{id}}} = 0$ we obtain

$$\mathrm{H}_{\max}^{\sqrt{2\epsilon}} (X|BC)_\omega \leq \mathrm{H}_{\max}^{\sqrt{2\epsilon}} \left(X|X'\right)_\omega \leq \mathrm{H}_{\max}\left(X|X'\right)_{\mathbb{P}_{\mathrm{id}}} = 0 \ ,$$

where the data processing inequality (27) is applied in the first inequality. For any $\delta > 0$ we can find a cq-state $\bar{\omega}_{XBC} \in \mathcal{B}^{\sqrt{2\epsilon}}(\omega_{XBC})$ such that $\mathrm{H}_{\max}^{\sqrt{2\epsilon}} (X|BC)_\omega \geq \mathrm{H}_{\max}(X|BC)_{\bar{\omega}} - \delta$. Hence with Lemma C.4

$$\log |C| \geq \mathrm{H}_{\max}(X|B)_{\bar{\omega}} - \delta \geq \mathrm{H}_{\max}^{\sqrt{2\epsilon}} (X|B)_\omega - \delta \ ,$$

where the last inequality is due to $\mathcal{P}(\omega_{XB}, \bar{\omega}_{XB}) \leq \sqrt{2\epsilon}$. Because this holds for all $\delta > 0$ we found the desired result. □

9. Quantum Key Distillation

In quantum key distribution, one considers a tripartite information theoretical setting with parties Alice, Bob, and Eve. The goal is for Alice and Bob to create a key, that is, an uniformly distributed random bit string which is known to both of them (correctness condition), but not to the adversary Eve (security condition). There is an enormous number of ideas and corresponding implementations how to achieve this task (see [80] and references therein). Some implementations use systems that are known to be modeled correctly by finite-dimensional Hilbert spaces, and some do not. The latter are often called continuous variable quantum key distribution schemes. For these schemes theoretical difficulties arise [80, 55].

Here we do not analyze any quantum key distribution schemes in particular, but give an abstract quantification of the distillable key, as it was done in [35, 70] for the finite-dimensional case. A way to think about quantum key distribution is the following.[27] One commences with two space like separated parties Alice and Bob, which initially share a state $\omega_{AB} \in \mathcal{S}(\mathcal{M}_{AB})$ on a quantum system with an associated observable algebra $\mathcal{M}_{AB} = \mathcal{M}_A \vee \mathcal{M}_B$, where $\mathcal{M}_A$ is Alice's part and $\mathcal{M}_B$ Bob's part. Note that in contrast to the previous sections, $\mathcal{M}_A$ denotes a general von Neumann algebra, not a finite-dimensional one. Now it is assumed that the third party, Eve, does not have access to Alice's and Bob's system, i.e. all of Eve's measurement operators have to commute with all elements in $\mathcal{M}_{AB}$. This can be modeled by taking a purification ω_{ABE} of ω_{AB} and assuming that Eve has the complementary system $\mathcal{M}_E$ (cf. Definition 3.3).[28] The first step is then for Alice to apply a POVM $\{E_A^x\}_{x\in X} \subset \mathcal{M}_A$ with finite alphabet size $|X|$ to make her system classical (cf. Section 3.2). Thus the resulting post-measurement state is modeled by a cq-state $\omega_{XBE} \in \mathcal{S}(\ell^\infty(X) \otimes \mathcal{M}_{BE})$.

A one-way classical communication key distillation protocol for ω_{XBE} consists of a classical encoding map $\mathcal{E} : \ell^1(X) \to \ell^1(K_A)$ on Alice's side, sending a classical message M from Alice to Bob, and a decoding map $\mathcal{D} : \ell^1(M) \otimes \mathcal{N}(\mathcal{M}_B) \to \ell^1(K_B)$ on Bob's side, where $|K_A| = |K_B| = |K|$. An output state which provides a perfectly secure key corresponds to a uniform distribution on K_A, K_B

[27] The entanglement based approach presented in the following is also called quantum key distillation. Note that prepare and measure schemes can sometimes be analyzed in this approach as well (see [9] for a finite-dimensional example).

[28] As pointed out in Section 3.2, purifications do always exist, but are in general not unique. However, since they are all related by partial isometries (Lemma 3.4), it does not matter which one we use.

which is independent of the eavesdropper's information (which includes the classical message M), that is, a cccq-state

$$\frac{1}{|K|}e_{K_A} \otimes \frac{1}{|K|}e_{K_B} \otimes \omega_{ME} \ ,$$

where $e_K = (1, \ldots, 1) \in \ell^1(K)$, and $\omega_{ME} \in \mathcal{S}(\ell^\infty(M) \otimes \mathcal{M}_E)$ containing the classical message M and the quantum part $\mathcal{M}_E$.

Definition 9.1. *Let $\mathcal{M}_{BE}$ be a bipartite von Neumann algebra, X a set of finite cardinality, $\omega_{XBE} \in \mathcal{S}(\ell^\infty(X) \otimes \mathcal{M}_{BE})$, and $\epsilon > 0$. A one-way classical communication key distillation protocol for ω_{XBE} as defined above is called ϵ-secure with respect to $\mathcal{M}_E$, if the output state $\omega_{K_A K_B ME}$ of the protocol satisfies that*

$$\|\omega_{K_A K_B ME} - \frac{1}{|K|}e_{K_A} \otimes \frac{1}{|K|}e_{K_B} \otimes \omega_{ME}\|_{\ell^1(\mathcal{N}(\mathcal{M}_E))} \leq \epsilon \ . \tag{60}$$

The goal is to quantify the maximal achievable key length $|K|$ for given ω_{XBE} and $\epsilon > 0$.

Theorem 9.2. *Let $\mathcal{M}_{BE}$ be a bipartite von Neumann algebra, X a set of finite cardinality, $\omega_{XBE} \in \mathcal{S}(\ell^\infty(X) \otimes \mathcal{M}_{BE})$, and $\epsilon_1, \epsilon_2 > 0$. Then there exists a one-way classical communication key distillation protocol for ω_{XBE} that is $(\epsilon_1 + \epsilon_2)$-secure with respect to $\mathcal{M}_E$, and*

$$|K| = \left\lfloor \sup_{X \to (Y,Z)} 2^{\mathrm{H}_{\min}^{\epsilon_1/5}(Y|EZ)_\omega - \mathrm{H}_{\max}^{\epsilon_2/4}(Y|BZ)_\omega - 2\log\left(\frac{80}{\epsilon_1 \epsilon_2}\right)} \right\rfloor \ , \tag{61}$$

where the supremum is over all functions from X to a pair of random variables (Y, Z). Furthermore, for every one-way classical communication key distillation protocol for ω_{XBE} that is ϵ-secure with respect to $\mathcal{M}_E$ holds that

$$|K| \leq \sup_{X \to (Y,Z)} 2^{\mathrm{H}_{\min}^{\sqrt{2\epsilon}}(Y|EZ)_\omega - \mathrm{H}_{\max}^{\sqrt{2\epsilon}}(Y|BZ)_\omega} \ . \tag{62}$$

Proof. Since the idea for the proof is the same as in the finite-dimensional case [70], and moreover, the necessary generalizations to the von Neumann algebra setting are already achieved in Section 7 and 8, we only sketch the proof. In order to prove (61), we start by showing that a key length

$$2^{\mathrm{H}_{\min}^{\epsilon_1/5}(X|E)_\omega - \mathrm{H}_{\max}^{\epsilon_2/4}(X|B)_\omega - 2\log\left(\frac{80}{\epsilon_1 \epsilon_2}\right)} \tag{63}$$

is achievable. In a first step, Alice transmits her bit string X to Bob by sending a classical message M via the classical channel. Then, Alice and Bob perform privacy amplification on X, and thus, we have by Corollary 7.5 that

$$\mathrm{H}_{\min}^{\epsilon_1/5}(X|ME)_\omega - 2\log\frac{5}{\epsilon_1}$$

is achievable. In the following we estimate this quantity. For that we use a chain rule for the smooth conditional min-entropy (Lemma C.3) and Lemma C.5, to find that for any $\delta \geq 0$

$$\mathrm{H}_{\min}^{\delta}(X|ME)_\omega \geq \mathrm{H}_{\min}^{\delta}(XM|E)_\omega - \log|M| \geq \mathrm{H}_{\min}^{\delta}(X|E)_\omega - \log|M| \ .$$

Moreover by (58), classical data compression with quantum side information can be achieved for[29]

$$\log|M| = \mathrm{H}_{\max}^{\epsilon_2/4}(X|B)_\omega - 2\log\frac{16}{\epsilon_2} \ .$$

Putting all this together results in (63). If we allow Alice to perform preprocessing by computing Y, Z from X and sending Y to Bob via a classical channel, we finally find (61). The proof of (62) can be found in [70]. □

[29] We choose $\epsilon = \epsilon_2/2$ in (58), since the error measured in norm distance is then upper bounded by ϵ_2 (and not ε).

For particular quantum key distribution schemes, the power of Alice and Bob is often limited in the sense that they can only make some kind of measurements (but usually unlimited classical post-processing). That is, one is not interested in the theoretically optimal amount of distillable key, but to prove the security of a scheme at hand. Going back to equation (61), this means that one has to show that there is a non-zero ϵ-secure key rate, i.e. to show that

$$\mathrm{H}^{\epsilon}_{\min}(X|E)_{\omega} - \mathrm{H}^{\epsilon}_{\max}(X|X')_{\omega} > 0 \ , \tag{64}$$

where $\omega_{XX'}$ denotes the state hold by Alice and Bob, after Bob applied his local measurements. The max-entropy term can be estimated with a (classical) statistical analysis, because the relevant data is directly accessible to Alice and Bob. However, the difficult part is to estimate the min-entropy term which involves Eve's system, to which both, Alice and Bob, do not have access. The min-entropy term is then often estimated under the assumption that Eve only performs 'collective attacks'. In the finite-dimensional regime it is known that these collective attacks are qualitatively equal to general attacks, by means of the quantum exponential de Finetti theorem [72, 71] or the post-selection technique [27].[30] In contrast to this, it is known that these techniques do not work in the infinite dimensional case [26].[31] But very recently, a conceptually new proof technique for finite-dimensional systems was introduced in [92, 91]. It uses the entropic uncertainty relation with quantum side information (cf. Section 6) to estimate the min-entropy term in (64). The advantage is that no reference to the quantum exponential de Finetti theorem or the post-selection technique is necessary.[32] Thus, it seems to be promising to apply these ideas to continuous variable quantum key distribution schemes and a detailed analysis is work in progress.

10. Discussion and Outlook

We generalized the smooth entropy formalism to von Neumann algebras and established most of their important properties. This paves the way for applications of this formalism to quantum information theoretical tasks involving infinite-dimensional quantum systems. In particular, we considered the smooth conditional min- and max- entropy, $\mathrm{H}^{\epsilon}_{\min}(A|B)_{\rho}$ and $\mathrm{H}^{\epsilon}_{\max}(A|B)_{\rho}$, for the case when the system A is finite-dimensional (quantum or classical) and the system B is a general von Neumann algebra (Section 4). This also involved a discussion and extension of several tools from quantum information theory to the von Neumann algebra setting (Section 3). With this at hand, we proved several properties of these entropies, like the duality relation (Proposition 4.14) or an entropic uncertainty relation (Theorem 6.1). The operational interpretations shown in Sections 5 - 9, indicate that the smooth min- and max-entropy are really suitable entropic measures for general quantum systems.

We characterized two specific primitives in quantum information, namely, privacy amplification in Section 7 and data compression with quantum side information in Section 8. Both tasks address a situation where one aims to deduce the uncertainty about a classical system which is correlated to a quantum system. Hence, an interesting question that arises, is whether primitives in which both systems are quantum, like for instance quantum state merging [49, 48, 11] or decoupling properties [37, 36], also carry over to the setting of von Neumann algebras. Another question is if one recovers the von Neumann entropy in the asymptotic limit of an iid source. For the case where the system A and the system B are finite-dimensional, this was shown in [89], and then later generalized to the case when the system B is modeled on a separable Hilbert space [40].

As discussed in Section 9, the results in this paper might find applications for security proofs of continuous variable quantum key distribution schemes. In particular, all the basic operational tasks used in a generic quantum key distribution protocol, are now generalized to the setting of von Neumann algebras, which makes certain techniques presented in [72] also applicable for continuous

[30] Note however, that this step often makes practical implementations rather inefficient [81, 85].

[31] There exists attempts to introduce additional measurements to assure that the system in question can be modeled using finite-dimensional Hilbert spaces [73], which then make these techniques applicable.

[32] Therefore, this approach should be favored in the finite-dimensional case as well. In particular, it allows for a large class of protocols to calculate tight finite key rates that are unconditionally secure [91].

variable systems. In addition, we also generalized the uncertainty relation with quantum side information from [92] to the von Neumann algebra setting (Section 6), which is promising with regard to the new prove technique developed in [91]. This uncertainty relation might also be interesting on its own when applied to concrete physical systems, like for instance for position and momentum measurements.

It might also be enlightening to extend the scope of the smooth min- and max-entropy formalism to more general cases. For instance, the system A could be extended to continuous classical systems, which would lead to a regularized entropy density. This might be suitable to analyze measurement results of continuous variable systems, like the quadratures of a light field, and supersede technical problems which come along with a discretization of the measurement outcomes. Mathematically, one could also imagine to generalize the formalism to operator systems [63]. From a physical perspective, this would correspond to a restriction of the actual measurement allowed to 'read out' the quantum system.[33] For a task like data compression with quantum side information (Section 8), this would allow to constraint the actual quantum measurements at the decoder.

Since the smooth entropy formalism has also been applied to thermodynamics [33, 30], the generalization to the von Neumann algebra setting is also of interest from a physical perspective. Especially, as quantum mechanical systems of interest in thermodynamics often possess an infinite number of degrees of freedom.

Acknowledgments

We thank Renato Renner for suggesting this work and an instructive discussion about privacy amplification. We would also like to thank Marco Tomamichel for many insightful discussions about the smooth entropy formalism, and for detailed feedback on the first version of this paper. We gratefully acknowledge discussions with Matthias Christandl, Reinhard Werner, Michael Walter, and Joseph Renes. MB and VBS are both deeply grateful for the hospitality and the inspiring working environment at the Institut Mittag-Leffler in Djursholm, Sweden, where this work was started. MB is supported by the Swiss National Science Foundation (grant PP00P2-128455) and the German Science Foundation (grants CH 843/1-1 and CH 843/2-1). FF acknowledges support from the Graduiertenkolleg 1463 of the Leibniz Universität Hannover, and FF and VBS both acknowledge support by the BMBF project QUOREP as well as the DFG cluster of excellence QUEST.

Appendix A. Standard Form of von Neumann Algebras

Each von Neumann algebra admits a representation for which all states are simultaneously pure in the sense of Definition 3.3, that is, each state allows a vector representation. This representation is called a standard form of the von Neumann algebra and discussed in [87, Section IX].

Proposition A.1. [87, Section IX] *Let $\mathcal{M}$ be a von Neumann algebra. Then there exists a faithful representation π on a Hilbert space $\mathcal{H}$, a positive cone $\mathcal{P} \subset \mathcal{H}$ and an anti linear isometry J with $J^2 = \mathbb{1}$, such that $J\pi(\mathcal{M})J = \pi(\mathcal{M})'$, and $J\eta = \eta$ for all $\eta \in \mathcal{P}$. Moreover, for each $\omega \in \mathcal{N}^+(\mathcal{M})$ there exists a unique $|\xi_\omega\rangle \in \mathcal{P}$ such that $\omega(x) = \langle \xi_\omega, \pi(x)\xi_\omega \rangle$ for all $x \in \mathcal{M}$.*

Definition A.2. *A representation of $\mathcal{M}$ as given in Proposition A.1 is called a standard form of $\mathcal{M}$ and specified by $(\mathcal{M}, H, \mathcal{P}, J)$, where we identified $\pi(\mathcal{M})$ with $\mathcal{M}$.*

The standard form of a von Neumann algebra is unique up to unitary equivalence [87, Section IX, Theorem 1.14].

[33] This restriction could also be conducted at a fundamental level, when one only excludes the elements of the von Neumann algebra that are unphysical in the sense that they do not correspond to a physical measurement.

Appendix B. Non-Commutative Radon-Nikodym Derivatives

This appendix is devoted to a short introduction into the concept of non-commutative Radon-Nikodym derivatives, which are generalizations of measure theoretic concepts to von Neumann algebras. However, in the following we do not assume any knowledge of classical results. The first non-commutative versions are due to Sakai [79].

Definition B.1. *Let $\mathcal{M}$ be a von Neumann algebra, $\omega, \sigma \in \mathcal{M}_+$, and $l \in \mathbb{R}^+$. We then call ω l-dominated by σ if*

$$\omega(a) \leq l \cdot \sigma(a) \ ,$$

holds for all $a \in \mathcal{M}$.

Proposition B.2. *Let $\mathcal{M}$ be a von Neumann algebra, and $\omega, \sigma \in \mathcal{N}^+(\mathcal{M})$ such that ω is l-dominated by σ. If $(\pi_\omega, \mathcal{H}_\omega, |\xi_\omega\rangle)$ and $(\pi_\sigma, \mathcal{H}_\sigma, |\xi_\sigma\rangle)$ are purifications of ω, σ, respectively, then there exists a positive operator h_ω on $\mathcal{H}_\sigma$, commuting with the range of π_σ, such that for all $a \in \mathcal{M}$*

$$\omega(a) = \langle \xi_\sigma \, | h_\omega \, \pi_\sigma(a) \, \xi_\sigma \, \rangle \ .$$

Moreover h_ω can be written as D^*D, where $D : \mathcal{H}_\sigma \to \mathcal{H}_\omega$ is a bounded operator satisfying

$$D\xi_\sigma = \xi_\omega \ ,$$

and the norm $\log \|h_\omega\| = \log \|D\|^2$ is given by the max-relative entropy $\mathrm{D}_{\max}(\omega \,||\, \sigma)$. The operator D is called the Radon-Nikodym derivative of ω with respect to σ.

Proof. Remember that we can assume that the purifications $(\pi_\omega, \mathcal{H}_\omega, |\xi_\omega\rangle)$ and $(\pi_\sigma, \mathcal{H}_\sigma, |\xi_\sigma\rangle)$ are cyclic, that is, we have $\mathcal{H}_\omega = \overline{\pi_\omega(\mathcal{M})|\xi_\omega\rangle}$ and likewise $\mathcal{H}_\sigma = \overline{\pi_\sigma(\mathcal{M})|\xi_\sigma\rangle}$. Hence, we can use ω to define a bounded positive bilinear form B on $\mathcal{H}_\sigma$ by the formula

$$B(\pi_\sigma(a)\xi_\sigma, \pi_\sigma(b)\xi_\sigma) = \omega(a^*b) \ .$$

By the representation theorem for bounded positive bilinear forms on a Hilbert space, there exist a unique operator h_ω on $\mathcal{H}_\sigma$ such that $B(\pi_\sigma(a)\xi_\sigma, \pi_\sigma(b)\xi_\sigma) = \langle \pi_\sigma(a)\xi_\sigma \, | h_\omega \, \pi_\sigma(b) \, \xi_\sigma \, \rangle$. Since ω is l-dominated by σ, we have that

$$\|h_\omega\| = \sup_{a \in \mathcal{M}} \frac{\langle \pi_\sigma(a)\xi_\sigma \, | h_\omega \, \pi_\sigma(a) \, \xi_\sigma \, \rangle}{\langle \pi_\sigma(a)\xi_\sigma \, | \pi_\sigma(a) \, \xi_\sigma \, \rangle} = \sup_{a \in \mathcal{M}} \frac{\omega(a^*a)}{\sigma(a^*a)} = \mathrm{D}_{\max}(\omega \,||\, \sigma) \ .$$

Next we have to check that h_ω is an element of $\pi_\sigma(\mathcal{M})'$. But this follows from the following simple computation. For $a, b, c \in \mathcal{M}$ we get

$$\begin{aligned} \langle \pi_\sigma(a)\xi_\sigma \, | h_\omega \pi_\sigma(b)\pi_\sigma(c)\xi_\sigma \, \rangle &= \langle \pi_\sigma(a)\xi_\sigma \, | h_\omega \pi_\sigma(bc)\xi_\sigma \, \rangle = \omega(a^*bc) \\ &= \langle \pi_\sigma(b^*a)\xi_\sigma \, | h_\omega \pi_\sigma(c)\xi_\sigma \, \rangle = \langle \pi_\sigma(a)\xi_\sigma \, | \pi_\sigma(b) h_\omega \pi_\sigma(c)\xi_\sigma \, \rangle \ , \end{aligned}$$

and hence, $[h_\omega, \pi_\sigma(b)] = 0$, $b \in \mathcal{M}$. Now define the operator D via $D\pi_\sigma(a)|\xi_\sigma\rangle = \pi_\omega(a)|\xi_\omega\rangle$ and due to the same argument as above it follows that D extends to a bounded operator satisfying $D\pi_\sigma(a) = \pi_\omega(a)D$ for all $a \in \mathcal{M}$ and $h_\omega = D^*D$. □

The following lemma is about the Radon-Nikodym derivative of cq-states.

Lemma B.3. *Let $\mathcal{M}_E$ be a von Neumann algebra, X a set of finite cardinality, $\omega_{XE} = \oplus_x \omega_E^x \in \ell^1(X) \otimes \mathcal{S}(\mathcal{M}_E)$, and $\tau \in \mathcal{N}^+(\mathcal{M}_E)$ such that $\omega_E^x \leq \tau$ for all $x \in X$. Furthermore, let $(\pi_\tau, \mathcal{H}_\tau, |\xi_\tau\rangle)$ be a purification of τ, and denote by D_x and D the corresponding Radon-Nikodym derivatives for ω_E^x and $\omega = \sum_{x \in X} \omega_E^x$ with respect to τ. Then it holds that*

$$\pi_\tau(a) \sum_{x \in X} D_x^* D_x \xi_\tau = \pi_\tau(a) D^* D \xi_\tau \ ,$$

for all $a \in \mathcal{M}_E$.

Proof. Since we can assume that the purification $(\pi_\tau, \mathcal{H}_\tau, |\xi_\tau\rangle)$ is cyclic, this follows easily because we have

$$\begin{aligned}\langle \pi_\tau(a)\xi_\tau \,|\pi_\tau(b) \sum_{x\in X} D_x^* D_x \xi_\tau \,\rangle &= \sum_{x\in X} \langle D_x\xi_\tau \,|\pi_\tau(a^*b) D_x\xi_\tau \,\rangle = \sum_x \omega_E^x(a^*b) = \omega(a^*b) \\ &= \langle \pi_\tau(a)\xi_\tau \,|\pi_\tau(b) D^*D\xi_\tau \,\rangle \ ,\end{aligned}$$

for all a, $b \in \mathcal{M}_E$. □

Appendix C. Misc Lemmata

The next two lemmata are the technical building blocks in the proof of Proposition 8.2.

Lemma C.1. [44, Lemma 2] *Let $\mathcal{M}$ be a von Neumann algebra, $S, T \in \mathcal{M}_+$, and $S \leq \mathbb{1}$. If $(S+T)$ is invertible in $\mathcal{M}$,*[34] *then it holds that*

$$\mathbb{1} - (S+T)^{-\frac{1}{2}} S (S+T)^{-\frac{1}{2}} \leq 2(\mathbb{1} - S) + 4T. \tag{65}$$

The following lemma was first proven in the finite-dimensional setting [5], and then generalized to von Neumann algebras [61].

Lemma C.2. *Let $\mathcal{M}$ be a von Neumann algebra, $\phi, \eta \in \mathcal{S}_\leq(\mathcal{M})$, s_+ the support projection onto the positive part of $\phi - \eta$, and $s_- = \mathbb{1} - s_+$. Then*

$$\phi(s_-) + \eta(s_+) \leq \mathcal{F}(\phi,\eta)^{\frac{1}{2}} \ . \tag{66}$$

Proof. The statement follows directly from [61, Corollary 1.1]. In order to see this we note that the relative modular operator $\Delta_{\eta,\phi}$ in a standard form $\{\mathcal{M}, \mathcal{H}, \mathcal{P}, J\}$ of $\mathcal{M}$ satisfies $\Delta_{\eta,\phi}|\xi_\phi\rangle = |\xi_\eta\rangle$ for $|\xi_\phi\rangle, |\xi_\eta\rangle \in \mathcal{P}$ purifications of ϕ and η, respectively. Hence, by the definition of the generalized fidelity

$$\|\Delta_{\eta,\phi}^{1/2} \xi_\phi\| = \langle \xi_\phi \,|\Delta_{\eta,\phi}\xi_\phi \,\rangle = \langle \xi_\phi \,|\xi_\eta \,\rangle \leq \mathcal{F}(\phi,\eta)^{\frac{1}{2}} \ .$$

Furthermore, we observe that

$$\begin{aligned}\phi(\mathbb{1}) + \eta(\mathbb{1}) - |\phi - \eta|(\mathbb{1}) &= \phi(\mathbb{1}) + \eta(\mathbb{1}) - (\phi-\eta)(s_+) + (\phi-\eta)(\mathbb{1}-s_+) \\ &= 2(\phi(s_-) + \eta(s_+)) \ .\end{aligned}$$

□

The following lemmata are needed in Section 9.

Lemma C.3. *Let $\mathcal{M}_{ABC} = M_m \otimes M_n \otimes \mathcal{M}_C$ with $\mathcal{M}_C$ a general von Neumann algebra, and $\omega_{ABC} \in \mathcal{S}(\mathcal{M}_{ABC})$. Then it follows that*

$$\mathrm{H}_{\min}^\epsilon(AB|C)_\omega \leq \mathrm{H}_{\min}^\epsilon(A|BC)_\omega + \log(n) \ .$$

Proof. The proof is the same as in the finite-dimensional case [70, Lemma 5]. For any $\delta_1 > 0$, there exists $\bar{\omega}_{ABC} \in \mathcal{B}^\epsilon(\omega_{ABC})$ such that $\mathrm{H}_{\min}^\epsilon(AB|C)_\omega \leq \mathrm{H}_{\min}(AB|C)_{\bar{\omega}} + \delta_1$, and for any $\delta_2 > 0$, there exists $\sigma_C \in \mathcal{S}(\mathcal{M}_C)$ such that $\mathrm{H}_{\min}(AB|C)_{\bar{\omega}} \leq -D_{\max}(\omega_{ABC}\|\tau_{AB} \otimes \sigma_C)$, where τ_{AB} denotes the trace on $M_m \otimes M_n$. Now we calculate

$$\begin{aligned}\mathrm{H}_{\min}^\epsilon(A|BC)_\omega + \log(n) &\geq \mathrm{H}_{\min}(A|BC)_{\bar{\omega}} + \log(n) \geq -D_{\max}(\bar{\omega}_{ABC}\|\tau_A \otimes \frac{\tau_B}{n} \otimes \sigma_C) + \log(n) \\ &= -D_{\max}(\bar{\omega}_{ABC}\|\tau_{AB} \otimes \sigma_C) \geq \mathrm{H}_{\min}(AB|C)_{\bar{\omega}} - \delta_2 \\ &\geq \mathrm{H}_{\min}^\epsilon(AB|C)_\omega - \delta_1 - \delta_2 \ ,\end{aligned}$$

and since that holds for any $\delta_1, \delta_2 > 0$, the claim follows. □

Lemma C.4. *Let $\mathcal{M}_{ABX} = \mathcal{M}_n \otimes \mathcal{M}_B \otimes \ell^\infty(X)$ with $\mathcal{M}_B$ a general von Neumann algebra, X a set of finite cardinality, and $\omega_{ABX} \in \mathcal{S}_\leq(\mathcal{M}_{ABX})$. Then it follows that*

$$\mathrm{H}_{\max}(A|BX)_\omega \geq \mathrm{H}_{\max}(A|B)_\omega - \log|X| \ . \tag{67}$$

[34] In the finite-dimensional case this requirement can be neglected by taking the inverse on the support of $S+T$.

Proof. We follow the proof from the finite-dimensional case [70, Lemma 4], and express (67) in terms of the conditional min-entropy by means of the duality relation (Proposition 4.14). Let us write $\omega_{ABX} = (\omega^x_{AB})_{x\in X}$ and take a representation π of $\mathcal{M}_{AB}$ on some Hilbert space $\mathcal{H}$ for which each ω^x_{AB} admits a purification $|\xi_x\rangle \in \mathcal{H}$. We denote the complementary system by $\mathcal{M}_R$. It then follows that $|\xi\rangle = \sum_x |\xi_x\rangle \otimes |x\rangle \otimes |x\rangle$ in $\mathcal{H} \otimes \mathbb{C}^{|X|} \otimes \mathbb{C}^{|X|}$ is a purification of ω_{ABX}. Hence (67) turns into

$$\mathrm{H}_{\min}(A|RXX')_\omega \geq \mathrm{H}_{\min}(A|RX')_\omega - \log|X| \ , \tag{68}$$

with $\omega_{ABRXX'}$ the state corresponding to $|\xi\rangle$. Note that X, X' do not refer to classical systems anymore, but to a finite dimensional quantum system of dimension $|X|$. If we define $\omega^{x,x'}_{ABR}$ as the functional on $\mathcal{M}_{ABR}$ given by $a \mapsto \mathrm{Tr}(a|\xi_x\rangle\langle\xi_{x'}|)$ one finds that (68) is equivalent to

$$\mathrm{H}_{\min}(A|RX)_\omega \geq \mathrm{H}_{\min}(A|RX)_{\tilde\omega} - \log|X| \ ,$$

where $\omega_{ARX} = (\omega^{x,x'}_{AR})_{xx'}$ and $\tilde\omega_{ARX} = (\omega^{x,x'}_{AR}\delta_{x,x'})_{xx'}$. This inequality now follows from the definition of the conditional min-entropy (Definition 4.2) and the fact that $\omega_{ARX} \leq |X| \cdot \tilde\omega_{ARX}$. In order to see the latter property, note that for any positive $E = (E_{xx'})_{xx'} \in \mathcal{M}_{ARX}$ the matrix $M_E = \left(\omega^{x,x'}_{AR}(E_{xx'})\right)_{xx'}$ is positive, wherefore

$$\omega_{ARX}(E) = \mathrm{Tr}\left[(1)_{xx'} \cdot M_E\right] \leq \|(1)_{xx'}\| \cdot \mathrm{Tr}\left[M_E\right] = \|(1)_{xx'}\| \cdot \tilde\omega_{ARX}(E) \leq |X| \cdot \tilde\omega_{ARX}(E) \ ,$$

where $(1)_{xx'}$ denotes the matrix with all entries equal to 1. □

Lemma C.5. *Let $\mathcal{M}_{AXB} = M_n \otimes \ell^\infty(X) \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a general von Neumann algebra, X a set of finite cardinality $|X|$, and $\omega_{AXB} \in \mathcal{S}_\leq(\mathcal{M}_{AXB})$. Then it follows that*

$$\mathrm{H}^\epsilon_{\min}\left(AX|B\right)_\omega \geq \mathrm{H}^\epsilon_{\min}\left(A|B\right)_\omega \ . \tag{69}$$

Proof. For $\epsilon = 0$, the proof from [72, Lemma 3.1.9] is also valid for von Neumann algebras. For $\epsilon > 0$, we proceed as follows. For all $\delta > 0$, there exists a cq-state $\bar\omega_{AB} \in \mathcal{B}^\epsilon(\omega_{XB})$ such that $\mathrm{H}^\epsilon_{\min}\left(A|B\right)_\omega \leq \mathrm{H}_{\min}\left(A|B\right)_{\bar\omega} + \delta$. We then take a purification $(\mathcal{H}, \pi, |\xi\rangle)$ of ω_{AXB} such that there exists also a purification $(\mathcal{H}, \pi, |\eta\rangle)$ of $\bar\omega_{AB}$ in $\mathcal{H}$. Now, by the definition of the purified distance (Definition 4.7), we can even find a purification $|\eta\rangle$ of $\bar\omega_{AB}$ such that $\mathcal{P}_{\mathcal{M}_{AB}}(\omega_{AB}, \bar\omega_{AB}) = \mathcal{P}_{\mathcal{B}(\mathcal{H})}(|\xi\rangle, |\eta\rangle)$. Hence, if we denote by $\bar\omega_{AXB}$ the state induced by $|\eta\rangle$, we get that $\bar\omega_{AXB} \in \mathcal{B}^\epsilon(\omega_{AXB})$. We can then estimate

$$\mathrm{H}^\epsilon_{\min}\left(A|B\right)_\omega \leq \mathrm{H}_{\min}\left(A|B\right)_{\bar\omega} + \delta \leq \mathrm{H}_{\min}\left(AX|B\right)_{\bar\omega} + \delta \leq \mathrm{H}^\epsilon_{\min}\left(AX|B\right)_\omega + \delta \ ,$$

where we the result for $\epsilon = 0$. Since this holds for any $\delta > 0$, the proof is completed. □

References

[1] P. M. Alberti. A note on the transition probability over C*-algebras. *Letters in Mathematical Physics*, 7:25–32, 1983.

[2] U. L. Andersen, G. Leuchs, and C. Silberhorn. Continuous variable quantum information processing. *Laser & Photonics Reviews*, 4:337–354, 2010. arXiv:1008.3468v1.

[3] H. Araki. Relative entropy of states of von Neumann algebras. *Publications of the Research Institute for Mathematical Sciences*, 11(3):809–833, 1975.

[4] H. Araki and E. J. Woods. A classification of factors. *Publications Research Institute for Mathematical Science Series A*, 4:51–130, 1968.

[5] K. M. R. Audenaert, J. Calsamiglia, R. Munoz-Tapia, E. Bagan, L. Masanes, A. Acin, and F. Verstraete. Discriminating states: The quantum chernoff bound. *Physical Review Letters*, 98:160501, 2007. arXiv:quant-ph/0610027v1.

[6] H. Barnum, M. Nielsen, and B. Schumacher. Information transmission through a noisy quantum channel. *Physics Review A*, 57:4153–4175, 1998. arXiv:quant-ph/9702049v1.

[7] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[8] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.

[9] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell's theorem. *Physical Review Letters*, 68:557, 1992.

[10] C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.

[11] M. Berta. Single-shot quantum state merging. Master's thesis, ETH Zurich, 2008. arXiv:0912.4495v1.

[12] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner. The uncertainty principle in the presence of quantum memory. *Nature Physics*, 6:659, 2010. arXiv:0909.0950v4.
[13] M. Berta, M. Christandl, and R. Renner. The quantum reverse Shannon theorem based on one-shot information theory. 2009. arXiv:0912.3805v2.
[14] I. Bialynicki-Birula and L. Rudnicki. Entropic uncertainty relations in quantum physics. 2010. arXiv:1001.4668v1.
[15] F. Brandão and N. Datta. One-shot rates for entanglement manipulation under non-entangling maps. *IEEE Transactions on Information Theory*, 57:1754, 2009. arXiv:0905.2673v2.
[16] O. Bratteli and D. W. Robinson. *Operator Algebras and Quantum Statistical Mechanics 1*. Springer, 1979.
[17] O. Bratteli and D. W. Robinson. *Operator Algebras and Quantum Statistical Mechanics 2*. Springer, 1981.
[18] D. Buchholz, C. D'Antoni, and K. Fredenhagen. The universal structure of local algebras. *Communications in Mathematical Physics*, 111(1):123–135, 1987.
[19] Donald Bures. An extension of Kakutani's theorem on infinite product measures to the tensor product of semifinite W*-algebras. *Transactions of the American Mathematical Society*, 135:199–212, 1969.
[20] F. Buscemi and N. Datta. Distilling entanglement from arbitrary resources. *Journal of Mathematical Physics*, 51:102201, 2010. arXiv:1006.1896v2.
[21] F. Buscemi and N. Datta. General theory of assisted entanglement distillation. 2010. arXiv:1009.4464v1.
[22] F. Buscemi and N. Datta. The quantum capacity of channels with arbitrarily correlated noise. *IEEE Transactions on Information Theory*, 56:1447, 2010. arXiv:0902.0158v5.
[23] F. Buscemi and N. Datta. Entanglement cost in practical scenarios. *Physical Review Letters*, 106:130503, 2011. arXiv:0906.3698v3.
[24] J. L. Carter and M. N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18:143–154, 1979.
[25] M. Christandl. Private communication. 2011.
[26] M. Christandl, R. König, G. Mitchison, and R. Renner. One-and-a-half quantum de Finetti theorems. *Communications in Mathematical Physics*, 273:473, 2007. arXiv:quant-ph/0602130v4.
[27] M. Christandl, R. König, and R. Renner. Post-selection technique for quantum channels with applications to quantum cryptography. *Physics Review Letters*, 102:020504, 2009. arXiv:0809.3019v1.
[28] P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths. Information theoretic treatment of tripartite systems and quantum channels. 2010. arXiv:1006.4859v5.
[29] P. J. Coles, L. Yu, and M. Zwolak. Relative entropy derivation of the uncertainty principle with quantum side information. 2011. arXiv:1105.4865v1.
[30] O. Dahlsten, R. Renner, E. Rieper, and V. Vedral. Inadequacy of von Neumann entropy for characterizing extractable work. *New Journal of Physics*, 13:053015, 2011. arXiv:0908.0424v1.
[31] N. Datta. Max- relative entropy of entanglement, alias log robustness. *International Journal of Quantum Information*, 7:475, 2009. arXiv:0807.2536v4.
[32] N. Datta. Min- and max- relative entropies and a new entanglement monotone. *IEEE Transactions on Information Theory*, 55(6):2816, 2009. arXiv:0803.2770v3.
[33] L. del Rio, J. Aberg, R. Renner, O. Dahlsten, and V. Vedral. The thermodynamic meaning of negative entropy. 2010. arXiv:1009.1630v1.
[34] I. Devetak and A. Winter. Classical data compression with quantum side information. *Physical Review A*, 68(4):042301, 2003. arXiv:quant-ph/0209029v4.
[35] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum state. *Proceedings of Royal Society A*, 461:207, 2005. arXiv:quant-ph/0306078v1.
[36] F. Dupuis. *The Decoupling Approach to Quantum Information Theory*. PhD thesis, Université de Montréal, 2009. arXiv:1004.1641v1.
[37] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner. The decoupling theorem. 2010. arXiv:1012.6044v1.
[38] A. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, 1991.
[39] F. Furrer. Min- and max-entropies as generalized entropy measures in infinite-dimensional quantum systems. Master's thesis, ETH Zurich, 2009.
[40] F. Furrer, J. Aberg, and R. Renner. Min- and max-entropy in infinite dimensions. *Communications in Mathematical Physics*, 306(1):165–186, 2011. arXiv:1004.1386v1.
[41] A. Gilchrist, N. K. Langford, and M. A. Nielsen. Distance measures to compare real and ideal quantum processes. *Physical Review A*, 71:062310, 2005. arXiv:quant-ph/0408063v2.
[42] R. Haag. *Local Quantum Physics: Fiels, Particles, Algebras*. Springer, 1992.
[43] P. Hausladen and W. K. Wootters. A pretty good measurement for distinguishing quantum states. *Journal of Modern Optics*, 41(12):2385, 1994.
[44] M. Hayashi and H. Nagaoka. General formulas for capacity of classical-quantum channels. *IEEE Transactions on Information Theory*, 49(7):1753–1768, 2003. arXiv:quant-ph/0206186v4.
[45] F. Hiai, M. Ohya, and M. Tsukada. Sufficiency, KMS condition and relative entropy in von Neumann algebras. *Pacific Journal of Mathematics*, 96(1):99–109, 1981.
[46] F. Hiai and D. Petz. The proper formula for relative entropy and its asymptotics in quantum probability. *Communications in Mathematical Physics*, 143(1):99–114, 1991.

[47] E. Hänggi and R. Renner. Device-independent quantum key distribution with commuting measurements. 2010. arXiv:1009.1833.
[48] M. Horodecki, J. Oppenheim, and A. Winter. Partial quantum information. *Nature*, 436:673–676, 2005. arXiv:quant-ph/0505062v1.
[49] M. Horodecki, J. Oppenheim, and A. Winter. Quantum state merging and negative information. *Communications in Mathematical Physics*, 269:107, 2006. arXiv:quant-ph/0512247v1.
[50] M.-H. Hsieh and N. Datta. One-shot entanglement-assisted classical communication. 2011. arXiv:1105.3321v1.
[51] R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions. *Proceedings of 21st Annual ACM Symposium on Theory of Computing*, pages 12–24, 1989.
[52] M. Junge, M. Navascues, C. Palazuelos, D. Perez-Garcia, V. B. Scholz, and R. F. Werner. Connes' embedding problem and Tsirelson's problem. *Journal of Mathematical Physics*, 52:012102, 2011. arXiv:1008.1142v1.
[53] R. König, U. M. Maurer, and R. Renner. On the power of quantum memory. *IEEE Transactions on Information Theory*, 51(7):2391–2401, 2005. arXiv:quant-ph/0305154v3.
[54] R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory*, 55(9):4674–4681, 2009. arXiv:0807.1338v1.
[55] A. Leverrier, F. Grosshans, and P. Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, 81:062343, 2010. arXiv:1005.0339v2.
[56] L. Masanes, S. Pironio, and A. Acin. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Communications*, 2:238, 2011. arXiv:1009.1567v2.
[57] M. Mosonyi and N. Datta. Generalized relative entropies and the capacity of classical-quantum channels. *Journal of Mathematical Physics*, 50:072104, 2009. arXiv:0810.3478v4.
[58] M. Navascues, T. Cooney, D. Perez-Garcia, and I. Villanueva. A physical approach to Tsirelson's problem. 2011. arXiv:1105.3373v1.
[59] M. Navascues, S. Pironio, and A. Acin. Bounding the set of quantum correlations. *Physical Review Letters*, 98:010401, 2007. arXiv:quant-ph/0607119v2.
[60] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000.
[61] Y. Ogata. A generalization of the inequality of audenaert et al. 2010. arXiv:1011.1340v1.
[62] V. I. Paulsen. *Completely bounded maps and operator algebras*. Cambridge University Press, 2002.
[63] V. I. Paulsen, I. Todorov, and M. Tomforde. Operator system structures on ordered spaces. 2009. arXiv:0904.3783v2.
[64] V. I. Paulsen and M. Tomforde. Vector spaces with an order unit. *Indiana University Mathematics Journal*, 58(3):1319–1360, 2009. arXiv:0712.2613v4.
[65] D. Petz. Quasientropies for states of a von Neumann algebra. *Publications of the Research Institute for Mathematical Sciences*, 21(4):787–800, 1985.
[66] D. Petz. Properties of the relative entropy of states of von Neumann algebras. *Acta Mathematics Hungary*, 47(1-2):65–72, 1986.
[67] M. Reed and B. Simon. *Methods of Modern Mathematical Physics, Vol. I: Functional Analysis*. NewYork Academic Press, 1978.
[68] J. M. Renes and J.-C. Boileau. Conjectured strong complementary information tradeoff. *Physical Review Letters*, 103:020402, 2009. arXiv:0806.3984v2.
[69] J. M. Renes and R. Renner. Noisy channel coding via privacy amplification and information reconciliation. 2010. arXiv:1012.4814v1.
[70] J. M. Renes and R. Renner. One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys. 2010. arXiv:1008.0452v2.
[71] R. Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3:645, 2007. arXiv:quant-ph/0703069v1.
[72] R. Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6:1, 2008. arXiv:quant-ph/0512258v2.
[73] R. Renner and J. I. Cirac. de Finetti representation theorem for infinite dimensional quantum systems and applications to quantum cryptography. *Physical Review Letters*, 102:110504, 2009. arXiv:0809.2243v1.
[74] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. *Springer Lecture Notes in Computer Science*, 3378:407, 2005. arXiv:quant-ph/0403133v2.
[75] R. Renner and S. Wolf. Smooth Rényi entropy and applications. *Proceedings of IEEE International Symposium Information Theory*, page 233, 2004.
[76] R. Renner and S. Wolf. Simple and tight bounds for information reconciliation and privacy amplification. *Springer Lecture Notes in Computer Science*, 3788:199, 2005.
[77] R. Renner, S. Wolf, and J. Wullschleger. The single-serving channel capacity. *Proceedings of IEEE International Symposium on Information Theory*, pages 1424–1427, 2006.
[78] A. Rényi. On measures of information and entropy. *Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability*, pages 547–561, 1960.

[79] S. Sakai. A Radon-Nikodym theorem in W*-algebras. *Bulletin American Mathematical Society*, 71(1):149–152, 1965.
[80] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81:1301, 2009. arXiv:0802.4155v3.
[81] V. Scarani and R. Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical Review Letters*, 100:200501, 2008. arXiv:0708.0709v2.
[82] V. B. Scholz and R. F. Werner. Tsirelson's problem. 2008. arXiv:0812.4305v1.
[83] B. Schumacher. Quantum coding. *Physics Review A*, 51:2738–2747, 1995.
[84] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.
[85] L. Sheridan, T. P. Le, and V. Scarani. Finite-key security against coherent attacks in quantum key distribution. *New Journal of Physics*, 12:123019, 2010. arXiv:1008.2596v1.
[86] M. Takesaki. *Theory of Operator Algebras 1*. Springer, 2001.
[87] M. Takesaki. *Theory of Operator Algebras 2*. Springer, 2002.
[88] M. Takesaki. *Theory of Operator Algebras 3*. Springer, 2002.
[89] M. Tomamichel, R. Colbeck, and R. Renner. A fully quantum asymptotic equipartition property. *IEEE Transactions on Information Theory*, 55:5840–5847, 2009. arXiv:0811.1221v3.
[90] M. Tomamichel, R. Colbeck, and R. Renner. Duality between smooth min- and max-entropies. *IEEE Transactions on Information Theory*, 56:4674, 2010. arXiv:0907.5238v2.
[91] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. 2011. arXiv:1103.4130v1.
[92] M. Tomamichel and R. Renner. The uncertainty relation for smooth entropies. *Physical Review Letters*, 106:110506, 2011. arXiv:1009.2015v2.
[93] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover hashing against quantum side information. *Proceedings of IEEE Symposium on Information Theory*, pages 2703–2707, 2010. arXiv:1002.2436v1.
[94] B. S. Tsirelson. Some results and problems on quantum Bell-type inequalities. *Hadronic Journal Supplement*, 8:329, 1993.
[95] A. Uhlmann. The transition probability in the state space of a *-algebra. *Report on Mathematical Physics*, 9:273, 1976.
[96] M. Walter. Private communication. 2011.
[97] L. Wang and R. Renner. One-shot classical-quantum capacity and hypothesis testing. 2010. arXiv:1007.5456v1.
[98] M. N. Wegman and J. L. Carter. New hash functions an their use in authentication and set equality. *Journal of Computer and System Sciences*, 22:265–279, 1981.
[99] S. Wehner and A. Winter. Entropic uncertainty relations - a survey. *New Journal of Physics*, 12:025009, 2010. arXiv:0907.3704v1.
[100] S. Wiesner. Conjugate coding. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984. Originally written c. 1970 but unpublished.
[101] A. Winter. Quantum information: Coping with uncertainty. *Nature Physics*, 6:640, 2010.
[102] S. L. Woronowicz. On the purification of factor states. *Communications in Mathematical Physics*, 78:221–235, 1972.